Guia do Usuário da Central do Cliente

AbsoluteSoftware

www.absolute.com

Setembro 2015

Guía del Usuario del Centro de Clientes, versão 5.23 — Documentação Versão 1

Absolute Software Corporation,
Suite 1600 Four Bentall Centre
1055 Dunsmuir Street
PO Box 49211
Vancouver, British Columbia
Canada V7X 1K8

Para uma lista de patentes emitidas à Absolute Software Corporation, consulte www.absolute.com/patents.

Conteúdo da mensagem

Capítulo 1: Introdução

Desde 1993 que a Absolute Software tem ajudado empresas a superar os riscos de segurança e os desafios do gerenciamento de ativos associados à propriedade e manutenção de grandes números de dispositivos: remotos, móveis ou de escritório.

A plataforma de tecnologia da Central do Cliente é uma arquitetura cliente/servidor que entrega os produtos de segurança de dispositivos, segurança de dados e de gerenciamento de ativos, da Absolute Software, como produtos autônomos ou como parte de um pacote completo.

A comunicação entre o software de agente seguro e patenteado do Computrace e o Centro de Monitoramento garante que as empresas tenham acesso seguro a informações atualizadas sobre o seu inventário completo de tecnologias de informação (TI). Usuários autorizados podem usar as ferramentas incorporadas na Central do Cliente para rastrear dispositivos, criar relatórios de furto para dispositivos furtados e iniciar operações de recuperação de dados e dispositivos.

Este capítulo inclui informações sobre os seguintes tópicos:

Sobre este Guia

Este documento contém as instruções necessárias para administradores do sistema a acessar o aplicativo da Central do Cliente usando um navegador Web para:

- Gerenciar ativos e gerar relatórios.
- Relatar um furto (disponível apenas a clientes de Computrace®Plus, Computrace Complete ou Computrace One™).
- Iniciar a Recuperação Remota de Arquivos, a Exclusão de Dados e o Congelamento de Dispositivo (disponível apenas para clientes pré-autorizados do ComputracePlus, Computrace Complete, Computrace®Data Protection, ou Computrace One).
- Configurar e administrar contas de usuários.
- Configurar informações de ativos e de usuário.

Este guia inclui informações detalhadas sobre as diversas ferramentas e funcionalidades disponíveis a usuários autorizados.

Alguns recursos podem não estar disponíveis na sua conta, dependendo do produto da Central do Cliente que sua empresa adquiriu. Para mais informações sobre vários produtos, consulte "Níveis de Serviço" na página 20.

Esta seção oferece informações acerca dos seguintes tópicos:

Público-alvo

Este guia fornece instruções para administradores de sistemas que usam a Central do Cliente para gerenciar seus ativos de TI (dispositivos), para relatar dispositivos perdidos ou furtados e para solicitar e monitorar operações de segurança de dados e dispositivos. Administradores de sistemas são atribuídos às funções de usuário de Administrador de Segurança ou Administrador, dependendo dos requisitos específicos das suas empresas.

Funções de Usuário da Central do Cliente

A Central do Cliente tem funções de usuário distintas que podem ser preenchidas por uma ou mais pessoas.

- **Administradores** gerenciam os dispositivos e ativos de TI das suas empresas e relatam furtos e perdas de dispositivos. Administradores também criam e gerenciam várias comunicações de sistema, tais como mensagens do usuário final, notificações do sistema e alertas e eventos de alerta suspeitos.
- **Administrador de Segurança** existem naquelas empresas que decidem designar certos administradores como Administrador de Segurança para gerenciar a segurança de dispositivos e de dados de ativos. Esta função de usuário tem mais direitos de acesso que os Administradores.

  Os administrador de segurança possuem a autoridade para configurar, selecionar e iniciar serviços de Recuperação de Arquivos, de Congelamento de Dispositivo e de Exclusão de Dados. Os Administradores de Segurança usam a Central do Cliente para rastrear e gerenciar dispositivos, tanto dentro da rede local da empresa como fora da mesma.
- **Usuários Avançados** têm direitos de acesso para a maioria de recursos da Central do Cliente, excluindo recursos de segurança. Administradores podem restringir os direitos de Usuários Avançados a identificadores ou grupos de dispositivos específicos.
- **Usuários de Segurança Avançados** existem naquelas empresas que decidem designar certos Usuários Avançados como Usuários de Segurança Avançados para gerenciar a segurança de dispositivos e de dados de ativos. Esta função de usuário tem mais direitos de acesso que os Usuários Avançados.

  Os Usuários de Segurança Avançados são autorizados a configurar, selecionar e iniciar serviços de Recuperação de Arquivos, de Congelamento de Dispositivo e de Exclusão de Dados em dispositivos no Grupo de Dispositivos atribuído a eles. Os Usuários de Segurança Avançados usam a Central do Cliente para rastrear e gerenciar dispositivos dentro da rede local da empresa.
- **Usuários Convidados** têm acesso limitado a informação e a relatórios da Central do Cliente. Estes usuários não podem alterar ou atribuir direitos de acesso a usuários nem podem alterar detalhes na página. Membros do Grupo de Usuários Convidados só podem navegar pelos Relatórios de Furto que eles próprios criaram e só podem visualizar relatórios que eles próprios salvaram.

Para mais detalhes sobre cada função de usuário da Central do Cliente, consulte o seguinte tópico: "Funções de usuário e seus direitos de acesso" na página 1.

Outras Funções de Usuário

As seguintes funções de usuário, apesar de não serem definidas na seção de Usuário na Central do Cliente, são importantes para a operação total da Central do Cliente.

- **Oficiais Responsáveis** assumem responsabilidade para as ações dos Administradores de Segurança e dos Usuários de Segurança Avançados. Oficiais Responsáveis são notificados a cada vez que uma solicitação de uma Exclusão de Dados é feita.

  Oficiais Responsáveis são dois gerentes seniores em uma empresa que têm poderes de autorização em nome das suas empresas.
- **Técnicos Informáticos** são normalmente responsáveis pela instalação do agente Computrace em dispositivos dentro das suas empresas.

Como usar este guia

O Guia do Usuário da Central do Cliente é composto pelos seguintes capítulos:

- "Introdução" (este capítulo) fornece uma visão geral deste documento.
- "Trabalhando com a Central do Cliente" mostra os requisitos mínimos de hardware e software, descreve métodos para acessar a Central do Cliente, fornece informações sobre a home page, incluindo seus links e painel de controle e inclui tarefas relacionadas à funcionalidade de MeuPerfil.
- "Configurando a Central do Cliente para Seu Ambiente de Trabalho" descreve os recursos da Central do Cliente incluídos na seção Administração, incluindo procedimentos necessários para a configuração de alertas de eventos, departamentos, grupos de dispositivos, funções de usuário (e seus direitos de acesso) e outras informações sobre ativos.
- "Configurando a Central do Cliente para Seu Ambiente de Trabalho" descreve os procedimentos necessários para gerar relatórios básicos e personalizados com base nos dados coletados de seus dispositivos gerenciados.
- "Trabalhando com Relatórios" descreve todos os relatórios disponíveis na Central do Cliente e como executá-los e ver os resultados.
- "Usando a Tecnologia de Tempo Real" descreve o recurso de Tecnologia de Tempo Real (RTT) e fornece tarefas que são específicas ao uso do mesmo.
- "Usando a Tecnologia de Tempo Real sobre IP" descreve o recurso de Tecnologia de Tempo Real sobre Protocolo IP (RTT-IP) e fornece tarefas que são específicas ao uso do mesmo.
- "Protegendo seus dados e dispositivos" descreve serviços de segurança de dados e dispositivos que habilitam usuários com autorização de segurança a garantir que dispositivos gerenciados e seus dados não sejam comprometidos em casos de perda ou furto.
- "Concluindo o Suporte para a Intel Anti-Theft Tecnology" fornece informações para ajudá-lo a solucionar problemas com a desinscrição de seus dispositivos gerenciados do Intel ® AT na Central do Cliente. O serviço Intel AT foi descontinuado pela Intel no início de 2015.
- "Usando a Exclusão de Dados" descreve a funcionalidade da Exclusão de Dados e os procedimentos necessários para iniciar e gerenciar operações de Exclusão de Dados.
- "Gerenciando Cercas Geográficas" descreve a funcionalidade de Cercas Geográficas Virtuais e os procedimentos necessários para gerenciar os limites das cercas geográficas virtuais.
- "Usando o Congelamento de Dispositivo" descreve a funcionalidade de Congelamento de Dispositivo, incluindo como inicializar solicitações de congelamento e criar mensagens personalizadas de congelamento.
- "Usando Recuperação Remota de Arquivos" descreve a funcionalidade de Recuperação Remota de Arquivos.
- "Usando a Lista de Arquivos" descreve como solicitar uma Lista de Arquivos remotamente, que facilita a solicitação de uma Recuperação Remota de Arquivos.

- "Computrace Mobile Theft Management para dispositivos iPad" descreve como gerenciar dispositivos iPad e iPad mini na Central do Cliente, e como criar um relatório de furto para dispositivos iPad furtados.
- "Computrace Mobile Theft Management Mobile Theft Management para Dispositivos Chrome" descreve como gerenciar Chromebooks e Chromeboxes na Central do Cliente, e como criar um relatório de furto para dispositivos Chrome furtados.
- "Relatando o Furto de um Dispositivo Gerenciado" descreve os procedimentos usados para relatar a perda ou furto de ativos gerenciados, assim como visualizar e gerenciar relatórios de furto. Este capítulo também inclui uma lista de verificação para seguir quando você envia um relatório de furto e um formulário de envio da Garantia de Serviço à Absolute Software.
- "Glossário" fornece uma lista de acrônimos, bem como os termos e suas definições usados em todo este guia.

Convenções usadas neste Guia

As seguintes convenções são usadas em todo o Guia do Usuário da Central do Cliente:

- Nomes de diretórios, nomes de arquivos, nomes de campos e objetos de IU são representados usando negrito; por exemplo:
  - No Windows 7, o arquivo `notepad.exe` está localizado no diretório `windows\system32`.
  - **UserID**: digite o seu número de identificação de usuário neste campo.
  - Clique em **Aplicar**.
- Entradas e saídas processadas por computador, tais como código de amostra e comandos ou instruções são exibidos usando a fonte Courier; por exemplo:

  `lanmake ctinst.txt`
- Referências cruzadas para outros locais dentro deste guia de usuário são indicadas em texto verde com caracteres sublinhados; por exemplo: consulte Convenções usadas neste Guia. Clicando em uma referência cruzada leva você para esse local neste guia.
- Em todo este guia, chegando à pagina certa na Central do Cliente da maneira mais rápida é representado da seguinte forma:

  No painel de navegação, clique em **Segurança de Dados e Dispositivos**> **Autorização de Segurança** > **Solicitar Código de Autorização**.
- A saída gerada pela Central do Cliente, que é baseada nas informações que você digita na área Critérios de Pesquisa, é apresentada em uma área referida como a grelha de resultados. Para certos relatórios, se referem a estes dados de saída como dados de saída de relatório.
- Referências cruzadas para outros locais neste guia são expressadas de uma das seguintes maneiras:
  - Para mais informações, consulte o seguinte tópico: indica que há informações que fornecem mais contexto sobre este tópico.
  - Consulte a seguinte tarefa: indica onde encontrar instruções específicas.

Navegando pela Central do Cliente

A Central do Cliente fornece as seguintes ferramentas de navegação:

- Painel de Navegação
- Links da parte superior da página
- Os links da parte inferior da página

Painel de Navegação

Todas as páginas na Central do Cliente contêm um painel de navegação global à esquerda. Este painel contém links que permitem que você navegue de uma seção para outra com poucos cliques. Na parte superior direito do painel de navegação, faça o seguinte:

- Para ocultar o painel de navegação e ter uma visualização completa de qualquer página, clique em .
- Para mostrar o painel de navegação e restaurá-lo ao seu estado original, clique em .

O painel de navegação contém os seguintes links: A funcionalidade que a Central do Cliente fornece depende de sua conta e credenciais de usuário.

- **Início**: abre a Home page, que mostra o painel de navegação, os anúncios recentes, os widgets do Painel de controle, e, na parte inferior da página, links para Suporte e para Baixar Pacotes. Para mais informações sobre esta página, consulte "Home page da Central do Cliente" na página 27.
- **Relatórios**: abre a página Relatórios, que mostra e fornece links para os vários relatórios fornecidos pela Central do Cliente. Para informações sobre cada um destes relatórios, consulte "Trabalhando com Relatórios" na página 152.
- **Administração**: abre a página Administração, que mostra e fornece links para as várias tarefas administrativas, tais como a definição de alertas de eventos, a definição de funções de usuário e de informações sobre ativos e o gerenciamento de solicitações de auto-atendimento para a remoção de agentes Para mais informações sobre o que você pode fazer a partir desta página, consulte "Configurando a Central do Cliente para Seu Ambiente de Trabalho" na página 38.
- **Segurança de Dados e Dispositivos**: dependendo do que é aplicável à sua conta, os usuários com privilégios de autorização de segurança clicam neste link para abrir a página Segurança de Dados e Dispositivos onde eles realizam atividades de segurança tais como a Autorização de Segurança, a Exclusão de Dados, o Congelamento de Dispositivos, Lista de Arquivos e Recuperação Remota de Arquivos.

  Para mais informações sobre cada uma dessas atividades de segurança, consulte os seguintes tópicos:

  ○ "Protegendo seus dados e dispositivos" na página 258 (para Autorização de Segurança)
  ○ "Usando a Exclusão de Dados" na página 269
  ○ "Usando o Congelamento de Dispositivo" na página 303
  ○ "Usando a Lista de Arquivos" na página 339
  ○ "Usando Recuperação Remota de Arquivos" na página 333

- **Relatório de Furto**: abre o relatório de furto onde você cria, visualiza e edita arquivos de furto. Para mais informações, consulte "Relatando o Furto de um Dispositivo Gerenciado" na página 377.
- **Páginas Personalizadas** : permite a você acesso a quaisquer funções especiais disponíveis para a sua conta.

  NOTA O link para as **Páginas Personalizadas** e os conteúdos que ela fornece estão disponíveis apenas em contas com funcionalidades especialmente modificadas (compiladas sob contrato).

- **Documentação**: abre a página Documentação que fornece acesso a todos os documentos importantes da Central do Cliente.
- **Suporte**: abre a página do Suporte que fornece alguns links úteis, incluindo um link para o formulário para se entregar um processo de suporte. Para mais informações sobre como entregar um processo de suporte, consulte "Contatando o Suporte Global da Absolute Software" na página 23.

NOTA A maioria de tarefas neste guia de usuário se refere à utilização do painel de navegação para você chegar aonde quer ir porque essa é a maneira mais fácil. Há alturas, no entanto, quando você precisa abrir uma página em particular para chegar à página que deseja usar. Em tais casos, você é instruído a navegar em conformidade.

Links da parte superior da página

Na parte superior de cada página da Central do Cliente, os seguintes links fornecem acesso a vários recursos:

- **ID da Conta**: mostra a conta à qual você está conectado.
- **Nome de Usuário**: mostra o nome do usuário que está conectado.
- **Meu Perfil**: abre a página Gerenciar Perfil de Usuário para o usuário que está conectado. Para mais informações acerca da edição de seu perfil de usuário, consulte "Trabalhando com Seu Perfil de Usuário" na página 34.
- **Documentação**: fornece acesso a todos os documentos importantes da Central do Cliente.
- **Suporte**: abre a página do Suporte que fornece alguns links úteis e um formulário para preencher durante o envio de um processo de suporte. Para mais informações sobre como entregar um processo de suporte, consulte "Contatando o Suporte Global da Absolute Software" na página 23.
- **Sair**: desconecta você da Central do Cliente e leva você de volta para a página de login da Central do Cliente.

Os links da parte inferior da página

Todas as páginas na Central do Cliente também contêm os seguintes links na parte inferior da página:

- **Política de Privacidade**: abre uma página que descreve as políticas da Absolute Software que abrangem a coleção, o uso e a divulgação de informações pessoais que nós recebemos a partir de seu uso da Central do Cliente ou de outros serviços relacionados
- **Contrato de Serviço**: abre o Contrato de Serviço que descreve os termos do contrato entre a sua empresa e a Absolute Software
- **Absolute Software Corporation**: abre o site da Absolute Software

Níveis de Serviço

A Central do Cliente disponibiliza diferentes níveis de serviço, baseados no produto que você adquire. Para mais informações sobre os vários níveis de serviço e que tipo de funcionalidade os vários recursos fornecem em cada plataforma suportada, vá para www.absolute.com/en/resources/matrices/absolute-computrace.

Dependendo do nível de serviço adquirido, algumas funcionalidades e relatórios da Central do Cliente podem não estar disponíveis. Por exemplo, os relatórios do Absolute Track® e do Computrace Complete estão indisponíveis para clientes que só subscreveram ao Computrace Plus. Para mais informações sobre os relatórios disponíveis para os clientes do AbsoluteTrack, Computrace Complete, Computrace Data Protection e Computrace One, vá para www.absolute.com/en/resources/matrices/absolute-computrace.

Para comprar ComputracePlus, Computrace Mobile, Absolute Track, Computrace Data Protection ou Computrace Complete, contate o departamento de vendas da Absolute Software em sales@absolute.com.

O Computrace One está apenas disponível na região da Europa, Oriente Médio e África (EMEA). Para adquirir o Computrace One, entre em contato com o departamento de vendas EMEA da Absolute Software em sales@EMEA.absolute.com.

Compreendendo a Função do Agente Computrace

O agente Computrace é a parte da tecnologia da Absolute Software que reside em dispositivos gerenciados e permite que você monitore estes dispositivos na Central do Cliente. Depois do agente ser inicialmente instalado em um dispositivo novo, o agente é ativado com a primeira chamada para o Centro de Monitoramento da Absolute. Durante esta chamada de ativação, o Centro de Monitoramento atribui um identificador único ao dispositivo e cria um registro de banco de dados que contém detalhes sobre o dispositivo.

Todos os dados transmitidos entre o agente e o Centro de Monitoramento são criptografados usando criptografia AES baseada em GCM de 128 bits.

O agente Computrace é composto por duas componentes.

- O **Agente de Aplicativo** é software que se instala no sistema operacional (como um serviço) do dispositivo. O agente faz chamadas programadas regularmente pela Internet para o Centro de Monitoramento e fornece dados coletados sobre o dispositivo. O agente também gerencia os "aplicativos de auxílio" Absolute para suportar atividades como as ações de segurança de Exclusão de Dados ou para assistir na recuperação por furto.

  O agente é pequeno e leve, mas não é fácil removê-lo e não é possível removê-lo manualmente quando a Persistência Absolute está ativa.
- Quando ativa, a **Tecnologia de Persistência** é acionada durante a primeira chamada do agente para o Centro de Monitoramento. A Tecnologia de Persistência restaura o agente caso este esteja ausente, adulterado ou danificado. Por exemplo, se um ladrão furtar um laptop e reinstala o sistema operacional, a tecnologia de persistência restaura o agente.

Esta seção oferece informações acerca dos seguintes tópicos:

- Sobre Chamadas de Agente
- Status do Agente

- Plataformas Suportadas para o Agente Computrace
- Gerenciando o Agente Computrace

Sobre Chamadas de Agente

Uma chamada de agente é uma conexão segura que permite que o agente Computrace e o Centro de Monitoramento da Absolute comuniquem entre eles.

Um dispositivo pode realizar uma chamada de agente das seguintes formas:

- Chamadas Agendadas
- Chamadas de Eventos
- Chamadas Forçadas

Chamadas Agendadas

Após o agente Computrace ser instalado em um dispositivo e a chamada de ativação ser concluída, o agente automaticamente realiza chamadas agendadas regulares para o Centro de Monitoramento. Por padrão, uma chamada programada é feita uma vez por dia. Durante estas chamadas, os dados de dispositivos mais recentes são enviadas ao Centro de Monitoramento e as instruções para quaisquer operações de segurança pendentes, tais como a Exclusão de Dados, o Congelamento de Dispositivo ou a Recuperação Remota de Arquivos, são enviadas ao dispositivo.

Chamadas de Eventos

Para dispositivos do Windows e Mac ativos, é possível ligar o recurso de Chamadas de Eventos, que habilitará estes dispositivos a fazerem uma chamada de agente quando um evento específico ocorrer. Uma alteração a qualquer um dos atributos seguintes do dispositivo pode acionar uma chamada de eventos:

- localização de dispositivo
- configuração de hardware
- software instalado
- informação de rede
- usuário conectado

Chamadas de eventos suplementam as chamadas agendadas que ocorrem automaticamente a partir de cada dispositivo gerenciado a cada 24,5 horas. No entanto, quando ocorre um chamada de evento, ela redefine o agendamento de chamadas regular. Tipicamente, quando as chamadas de eventos estão ligadas, as informações de dispositivos na Central do Cliente estão mais atualizadas, o que significa que os alertas são acionados em uma base mais atempada e seus relatórios são mais precisos.

É possível ligar ou desligar as chamadas de eventos para todos os dispositivos do Windows ou do Mac dentro de uma conta ou para dispositivos gerenciados individuais.

Para mais informações sobre como gerenciar chamadas de eventos, consulte os seguintes tópicos:

- "Gerenciando Chamadas de Eventos para Sua Conta" na página 119
- "Editando Informações de Ativos" na página 141

Chamadas Forçadas

Para dispositivos com Windows equipados com a Tecnologia de Tempo Real (RTT), é possível enviar uma solicitação a partir da Central do Cliente para forçar o dispositivo a fazer uma chamada não agendada para o Centro de Monitoramento. Para mais informações, consulte os seguintes tópicos:

- "Usando a Tecnologia de Tempo Real" na página 242
- "Iniciando uma Chamada Forçada" na página 247

Status do Agente

Na Central do Cliente, o agente Computrace pode ser definido para um dos seguintes status:

- **Ativo** indica que o agente chamou para o Centro de Monitoramento.
- **Inativo** indica que o agente ainda não chamou para o Centro de Monitoramento.
- **Desativado** indica que o agente está sinalizado para remoção ou que foi removido do dispositivo.

É possível visualizar o status do agente de um dispositivo nos seguintes relatórios:

- Relatório de Ativos
- Relatório do Histórico de Chamadas

É também possível visualizar informações detalhadas sobre o agente de um dispositivo no separador Rastreamento de Chamadas na página Resumo do Dispositivo de dispositivo. Consulte "Editando Informações de Ativos" na página 141.

Plataformas Suportadas para o Agente Computrace

O agente Computrace é suportado nas seguintes plataformas:

- Sistemas Operacionais Windows®:
  - Windows 8.1 (requer o agente Computrace versão 932 ou superior)
  - Windows 8 (requer o agente Computrace versão 910 ou superior)
  - Windows 7
  - Windows Vista

  NOTA Windows RT 8.x não é suportado.

- Sistema Operacional Mac OS X® , versão 10.5 e superior
- Sistema Operacional Chrome OS™, versão 36 e superior

  O sistema operacional Chrome OS é suportado somente quando ele está executando em um computador Chromebook™ notebook ou um computador desktop Chromebox™.
- Sistemas Operacionais do Windows Mobile:
  - Windows Mobile 5.0
  - Windows Mobile 6.0, 6.1, 6.2 e 6.5

  NOTA Se seu dispositivo executa o sistema operacional Windows Mobile 5.0, você deve instalar o .NET Compact Framework 2.0 SP2 Runtime, que está disponível na Microsoft em: www.microsoft.com/en-us/download/details.aspx?id=17981.

- Sistema Operacional BlackBerry®, versão 4.5

- Sistema Operacional Android™, versão 2.3 e superior
- Sistema Operacional Apple® iOS, versões 6.1 e 7.1 (em dispositivos iPad® e iPad mini™ apenas)

Para mais informações sobre a compatibilidade Computrace para dispositivos iPad e iPad mini, consulte "Computrace Mobile Theft Management para dispositivos iPad" na página 345.

NOTA Para receber mais informações sobre suporte para o agente Computrace em sistemas operacionais baseados em Linux, tais como Ubuntu 14.04 LTS ou Debian® 7.x, contate o Suporte Global. Consulte "Contatando o Suporte Global da Absolute Software" na página 23.

Gerenciando o Agente Computrace

Na Central do Cliente é possível executar as seguintes tarefas relacionadas ao agente Computrace e às chamadas ele faz para o Centro de Monitoramento.

- Baixe a versão mais recente do agente para um dispositivo gerenciado. Consulte "Baixando o Agente Computrace" na página 127.
- Ver o histórico de chamadas de um ou mais dispositivos. Consulte "Relatório do Histórico de Chamadas" na página 208.
- Gerencie as chamadas de eventos para todos os dispositivos do Windows ou Mac associados a uma conta ou para dispositivos individuais. Para mais informações, consulte os seguintes tópicos:
  - "Gerenciando Chamadas de Eventos para Sua Conta" na página 119
  - "Editando Informações de Ativos" na página 141
- Forçar uma chamada em dispositivos com Windows equipados com a RTT. Consulte "Iniciando uma Chamada Forçada" na página 247.
- Solicitar uma operação de segurança em um dispositivo na próxima chamada do agente. Consulte "Protegendo seus dados e dispositivos" na página 258.
- Remover o agente de um dispositivo. Consulte "Gerenciando solicitações de remoção de agentes" na página 132.

Contatando o Suporte Global da Absolute Software

Se você tiver dificuldade ao usar a Central do Cliente ou ao instalar o agente, entre em contato com o Suporte Global da Absolute Software. Suas perguntas, comentários e solicitações de recursos são bem-vindos.

IMPORTANTE Para remover o agente de um ou mais dispositivos gerenciados, os administradores de segurança podem usar o recurso de auto-atendimento de remoção de agentes disponível na área de Administração. Para mais informações, consulte "Gerenciando solicitações de remoção de agentes" na página 132.

Para contatar o Suporte:

1. Conecte-se à Central do Cliente usando seu **Nome de Usuário** e **Senha**.
2. Clique no link **Suporte** no painel de navegação ou no topo de qualquer página na Central do Cliente.

3. Na área de Suporte Global, clique no link **Enviar um Caso de Suporte** para abrir a página Casos de Suporte no website do Suporte Global da Absolute.

4. Forneça os seguintes detalhes sobre o problema que você está enfrentando:
   - **Produto** identifica o produto a qual o problema se aplica, que neste caso é o **Computrace**.
   - **Tipo de Problema** encaminha o problema para os Representantes de Suporte apropriados para uma solução rápida e eficiente.
   - A **Severidade** ajuda o Suporte Global da Absolute Software a determinar a urgência e o impacto do problema. Para mais informações sobre os níveis de severidade e seus tempos de resposta correspondentes, clique no ícone ?.
   - O **Título** constitui o título da mensagem enviada ao Suporte Global da Absolute Software.
   - **Descrição** permite que você adicione informações detalhadas sobre o problema pelo qual você está entrando em contato com o Suporte Global da Absolute Software.
   - O/A**Código/Mensagem de Erro** permite que você adicione informações sobre quaisquer notificações do sistema, erros ou avisos que você possa ter encontrado juntamente com o problema.
   - Os **Anexos** permitem que você adicione quaisquer documentos ou imagens de auxílio para descrever mais o problema. Para a lista de formatos de arquivo aceites, focalize o mouse sobre **Ver tipos de arquivo suportados**.

   NOTA O tamanho de anexos não pode exceder 4096 Kilobytes (4 Megabytes ou MB) por anexo ou 12 MB no total.

5. Se o caso de suporte for de natureza confidencial ou sensível e você não quer que seja visível a terceiros, desmarque a caixa de seleção **Exibir este Caso de Suporte em Ver Casos de Suporte**.

6. Adicione suas **Informações de Contacto** e indique se preferia ser contatado por **E-mail** ou **Telephone**.

7. Clique em **Salvar Caso**.

   Uma mensagem que inclui informações sobre o seu problema é enviada para o Suporte Global da Absolute Software. Absolute Software O Suporte Global contatará você se mais informações forem necessárias e/ou quando uma solução para seu problema estiver disponível.

NOTA É também possível entrar em contato com o Suporte Global da Absolute Software em: www.absolute.com/support. Siga as instruções na tela para entrar em contato com o Suporte Global da Absolute Software de sua região.

Capítulo 2: Trabalhando com a Central do Cliente

Este capítulo faz uma apresentação da Central do Cliente e descreve a seguinte funcionalidade básica:

Requisitos do Sistema da Central do Cliente

Para usar a Central do Cliente, você precisa assegurar que seu computador cumpre os seguintes requisitos:

- **Acesso à Internet**: A Central do Cliente não está disponível no modo offline e o acesso à Internet é obrigatório.
- **Navegadores suportados**:
  - A Central do Cliente suporta as versões atuais e imediatamente anteriores dos seguintes navegadores:
    - Internet Explorer (Somente Windows)
    - Safari (apenas Mac)
  - A Central do Cliente suporta a versão atual do Google Chrome (Windows e Mac)
  - A Central do Cliente oferece *apenas suporte limitado*para as versões atuais dos seguintes navegadores:
    - Opera (Windows e Mac)
    - Firefox (Windows e Mac)

    NOTA Suporte para estes navegadores está limitado porque eles não são proativamente testados para compatibilidade com a Central do Cliente. No entanto, se clientes tiverem problemas ao usar a Central do Cliente nestes navegadores, faremos tudo dentro do possível para resolver estes problemas atempadamente.

- **Resolução da tela**: A resolução mínima suportada é a de 1024 x 768 pixels. As páginas da Central do Cliente são automaticamente redimensionadas para preencher telas de resoluções maiores.

Selecionando um Idioma

A Central do Cliente suporta os seguintes idiomas:

- Alemão
- Inglês
- Espanhol
- Italiano
- Japonês
- Coreano
- Turco
- Chinês (Simplificado)
- Chinês (Tradicional)

- Francês
- Português

Para selecionar um idioma, clique na lista de idiomas localizada na parte superior da página de Login. A pagina se atualiza e é apresentada no idioma escolhido. Para alterar o idioma escolhido na página de seu perfil de usuário, consulte "Editando Suas Configurações de Sistema do Usuário" na página 36.

NOTA Todas as páginas da Central do Cliente se expandem para acomodar as mudanças no tamanho do texto por conta da alteração do idioma.

Acessando a Central do Cliente pela Primeira Vez

Quando sua empresa adquire a Central do Cliente, a Absolute Software envia uma mensagem de e-mail para a configuração de conta para nosso ponto de contato em sua empresa. Esta mensagem inclui:

- seu número de conta
- um URL específico que permite que você acesse a Central do Cliente (tome nota do URL para usar quando quiser acessar a Central do Cliente novamente)
- um usuário de administração que está configurado para seu uso com um nome de usuário atual e uma senha para permitir que você se conecte a primeira vez

Se você tiver quaisquer perguntas ou necessitar de assistência, entre em contato com o Suporte Global Absolute como instruído na tarefa, "Contatando o Suporte Global da Absolute Software" na página 23.

Para acessar a Central do Cliente e conectar-se pela primeira vez:

1. Insira o URL específico de sua empresa de uma das seguintes formas:
   - Clique no link fornecido na mensagem de e-mail de configuração de conta para a Central do Cliente Absolute para abrir a página de login.
   - Se sua empresa fizer hospedagem de sua própria Central do Cliente, consulte seu administrador de sistemas para obter o URL correto para acessar a Central do Cliente.

   É provável que você queira apontar o endereço URL e consultá-lo sempre que necessário enquanto você se familiarizar com o aplicativo da Central do Cliente.
2. Na página de login da Central do Cliente, digite seu **Nome de Usuário** (não diferencia maiúsculas de minúsculas) e sua **Senha** (diferencia maiúsculas de minúsculas).

   Se você esqueceu de sua senha, antes de tentar conectar-se três vezes, siga as instruções na tarefa, "Recuperando uma Senha Esquecida" na página 27.

   IMPORTANTE Se você inserir sua senha incorretamente três vezes, poderá ver uma mensagem informando que seu login foi suspenso. Neste caso, entre em contato com o Suporte Global. Para mais informações, consulte "Contatando o Suporte Global da Absolute Software" na página 23.
3. Clique em **Entrar**. Se a combinação de seu nome de usuário e sua senha for correta, a home page da Central do Cliente será aberta.

Conectando-se à Central do Cliente

Para garantir que somente usuários autorizados tenham acesso aos dados de clientes, cada usuário registrado deve efetuar login para acessar a Central do Cliente.

Para conectar-se à Central do Cliente:

1. Acesse a Central do Cliente usando o URL específico de sua empresa.
2. Na página de login da Central do Cliente digite seu **Nome de Usuário** (não diferencia maiúsculas de minúsculas) e sua **Senha** (diferencia maiúsculas de minúsculas).

   Se você esqueceu de sua senha, antes de tentar conectar-se três vezes, siga as instruções na tarefa, "Recuperando uma Senha Esquecida" na página 27.

   IMPORTANTE Se você inserir sua senha incorretamente três vezes, poderá ver uma mensagem informando que seu login foi suspenso. Neste caso, entre em contato com o Suporte Global. Para mais informações, consulte "Contatando o Suporte Global da Absolute Software" na página 23.

3. Clique em **Entrar**.

   Se a combinação de seu nome de usuário e sua senha for correta, a home page da Central do Cliente será aberta.

Recuperando uma Senha Esquecida

Se você esqueceu sua senha e seu login não foi suspenso, você pode obter uma nova senha, que é descrito a seguir. No entanto, se você foi suspenso, consulte "Ativando um usuário suspenso" na página 114.

Para redefinir uma senha esquecida:

1. Abra a página de login da Central do Cliente.

   IMPORTANTE Se necessitar o URL correto para sua conta, entre em contato com o Suporte Global. Para mais informações, consulte "Contatando o Suporte Global da Absolute Software" na página 23.

2. Na página de login, clique no link de **Esqueceu sua Senha?** para abrir a página Recuperação de Senhas.
3. No campo **Usuário**, digite seu nome de usuário.
4. No campo **E-mail**, digite o endereço de e-mail associado ao seu nome de usuário.
5. Clique em **Enviar**.

   Uma nova senha é enviada ao endereço de e-mail associado ao seu nome de usuário.

Home page da Central do Cliente

Depois de você entrar com sucesso, a home page da Central do Cliente se abre. A partir desta página você pode juntar informações de conta pertinentes, tais como mensagens, itens de ação e um resumo de atividades em uma única visão.

Os conteúdos desta página são dinâmicas, com base em sua função de usuário e seus direitos de acesso. Administradores e administradores de segurança vêem o painel de controle, enquanto usuários de segurança avançado, usuários avançados e convidados não o vêem.

Em alguns casos, após você efetuar o login, uma caixa de diálogo de Anúncios abre para informar você de itens que precisam de sua atenção imediata.

Esta seção fornece as seguintes informações e tarefas:

- Diálogo de Anúncios
- Anúncios Recentes
- Resumo da Conta
- O Painel de controle e Seus Widgets

Diálogo de Anúncios

Em alguns casos, uma pequena tela inicial ou caixa de diálogo aparece após login bem-sucedido. A caixa de diálogo de Anúncios fornece uma lista de todos os itens de ação que precisam de sua atenção imediata, incluindo itens específicos a você, à sua conta na Central do Cliente, e aos produtos Absolute usados em sua conta.

O diálogo de anúncios é onde você executa as seguintes tarefas:

- Reconhecendo Anúncios
- Descartando Mensagens
- Fechando a Caixa de Diálogo de Anúncios sem Reconhecer os Anúncios

Reconhecendo Anúncios

Para dar reconhecimento de anúncios e fechar o diálogo:

1. Conecte-se à Central do Cliente. A home page da Central do Cliente se abre e um diálogo de anúncios aparece.
2. Clique em **OK** para dar reconhecimento de todos os anúncios que aparecem no diálogo.

   NOTA Quando você clica em **OK**, os anúncios são marcados como concluídos e a caixa de diálogo de Anúncios não abre novamente para essas mensagens. No entanto, sempre que houver um novo anúncio que se aplique a você ou a sua conta da Central do Cliente, o diálogo de anúncios se abre novamente a próxima vez que você se conectar à Central do Cliente.

3. Clique em ☒ para fechar a caixa de diálogo.

Descartando Mensagens

IMPORTANTE A caixa **Não mostrar novamente** está disponível apenas para mensagens não obrigatórias.

Para descartar mensagens não obrigatórias:

1. Conecte-se à Central do Cliente. A home page da Central do Cliente é aberta e um diálogo de anúncio aparece.
2. Marque a caixa de seleção **Não mostrar novamente**.

Esta ação indica que você deu reconhecimento aos anúncios, mas não que você os aceitou. Os anúncios são exibidos novamente a próxima vez que você se conectar à Central do Cliente.

3. Remova os anúncios da lista e clique em ☒ para fechar o diálogo.

   A caixa de diálogo de Anúncios poderá abrir-se a próxima vez que você entrar na Central do Cliente, mas as mensagens para as quais você marcou a caixa de seleção **Não mostrar novamente** não aparecerão novamente no diálogo de Anúncios.

Fechando a Caixa de Diálogo de Anúncios sem Reconhecer os Anúncios

Para fechar a caixa de diálogo, independentemente das mensagens mostradas:

1. Conecte-se à Central do Cliente. A home page da Central do Cliente se abre e um diálogo de anúncios aparece.

2. Clique em ☒ para fechar o diálogo sem dar reconhecimento dos anúncios que são exibidos.

   A próxima vez que você se conectar à Central do Cliente, a caixa de diálogo se abrirá para mostrar essas mensagens novamente.

Anúncios Recentes

A área dos **Anúncios Recentes** da home page mostra quaisquer mensagens importantes e fornece, ou oculta, uma lista das mensagens importantes mais recentes da Absolute Software Global Suporte que se aplica à sua conta ou ao seu perfil de usuário.

Para exibir uma lista de anúncios, faça uma das seguintes ações:

- Clique em **Anúncios Recentes**.
- Clique no link **Mostrar Detalhes**.
- Clique.

Para ocultar uma lista de anúncios, faça uma das seguintes ações:

- Clique em **Anúncios Recentes**.
- Clique no link **Ocultar Detalhes**.
- Clique.

Resumo da Conta

Para Usuários Avançados e Convidados, a área de **Resumo para a Conta** da homepage fornece uma visão geral de informações sobre a licença de produtos para a conta.

A área é dividida em três seções:

Seção	Detalhes
Produto / **Licença**	O número de licenças adquiridas para cada produto e o número total de licenças para sua conta.

Seção	Detalhes
Instalação / Detalhes da Chamada	Fornece informações sobre as licenças de agentes Computrace instaladas em dispositivos em sua conta. Para mais informações sobre o agente Computrace, consulte "Compreendendo a Função do Agente Computrace" na página 20. Esta seção inclui a seguinte informação: ● **Instalações em Excesso (-) ou a Menos (+)**: indica se a conta tem instalações em excesso ou a menos em relação ao número total de licenças de agentes Computrace ● **Total de Instalações**: mostra o número total de dispositivos com o agente Computrace instalado ● **Chamadas dos Últimos 30 Dias**: mostra o número total de dispositivos que fizeram chamadas para o Centro de Monitoramento nos últimos 30 dias ● **Taxa de Chamadas Recebidas Recentes**: exprime o valor para **Chamadas nos Últimos 30 Dias** como um percentual de **Total Instaladas**
Subconjunto de Garantia de Serviço	Fornece informações sobre dispositivos com a Garantia de Serviço. Para mais informações, consulte "Gerenciando Licenças da Garantia de Serviço" na página 125. Esta seção inclui a seguinte informação: ● **Garantia de Serviço Instalada (sinalizador definido):** mostra o número total de dispositivos com um sinalizador definido para a Garantia de Serviço ● **Instalações em Excesso (-) ou a Menos (+)**: indica se a conta tem instalações em excesso ou a menos em relação ao número total de licenças da Garantia de Serviço adquiridas ● **Taxa de Instalação:** exprime o valor para **Instalações em Excesso (-) ou a Menos (+)** como um percentual de toda as licenças do Garantia de Serviço adquiridas ● **Chamadas dos Últimos 30 Dias**: indica o número total de dispositivos com uma garantia de serviço que fizeram chamadas para o Centro de Monitoramento nos últimos 30 dias ● **Taxa de Chamadas Recebidas Recentes**: exprime o valor para **Chamadas nos Últimos 30 Dias** como um percentual de **Garantia de Serviço Instalada (sinalizador definido)**

O Painel de controle e Seus Widgets

Para administradores e administradores de segurança, a área do **Painel de controle** da home page mostra widgets em uma interface gráfica que fornece informações importantes relacionadas com a sua conta. Alguns widgets mostram informações na forma de um gráfico de pizza. Focalize o mouse sobre as unidades no gráfica de pizza para ver seus valores.

Esta seção fornece as seguintes informações e tarefas:

- Visualizando os Widgets que Aparecem quando Você se Conectar pela Primeira Vez
- Usando widgets
- Mostrando ou Ocultando Widgets Específicos
- Personalizando Widgets

Visualizando os Widgets que Aparecem quando Você se Conectar pela Primeira Vez

Quando você se conectar à Central do Cliente pela primeira vez, os seguintes widgets estão disponíveis no painel de controle:

- **Taxa de Chamadas do Agente (Todas)** mostra as estatísticas de chamadas do agente para todos os dispositivos. Clique no período de chamada desejado para abrir o Relatórios de Ativos com os intervalos de datas específicos pré-preenchidos no campo **Chamada mais recente**.
- **Produtos Ativos** mostra os produtos Computrace que estão ativos para os dispositivos na sua conta. Os produtos estão associados com Níveis de Serviço, que condicionam a funcionalidade disponível para dispositivos e grupos específicos. Para mais informações, consulte "Níveis de Serviço" na página 20.

  Você não pode fechar este widget.
- **Resumo de Licenças** mostra as licenças disponíveis na sua conta, em comparação com o número de licenças em uso atualmente. Clicando em um tipo de licença abre a lista de dispositivos que usam atualmente essas licenças.

  Você não pode fechar este widget.
- **Versões do Agente** mostra os números de versão dos diversos agentes em seus dispositivos gerenciados. Clique no número da versão desejada para abrir a página Relatório de Ativos com o número da versão selecionado pré-preenchido no campo **Versão do Agente**.
- **Resumo Antimalware** mostra um resumo dos dispositivos da sua conta que contêm produtos antimalware detectados e dispositivos sem qualquer produto antimalware. Os seguintes cenários são possíveis:
  - Para abrir o relatório de antimalware em falta, clique na área rotulada **Antimalware em Falta**.
  - Para abrir o Relatório de Anti-malware com o aplicativo específico ou o nome do fornecedor pré-preenchido no campo **Software Anti-malware**, clique no nome do produto anti-malware aplicável.

É também possível abrir os seguintes widgets se aplicável na sua conta, como descrito na tarefa, "Mostrando ou Ocultando Widgets Específicos" na página 32.

- **Taxa de Chamadas do Agente (Garantia de Serviço)** mostra estatísticas de chamadas do agente para dispositivos na sua conta com uma Garantia de Serviço. Clique no período de chamada desejado para abrir o Relatórios de Ativos com os intervalos de datas específicos pré-preenchidos no campo **Chamada mais recente**.
- **Relatórios Favoritos** pode ser personalizado para mostrar os cinco relatórios mais usados dos filtros de relatórios salvos na página **Meus Relatórios**. Clique no nome do relatório para abri-lo. Para mais informações, consulte "Usando widgets" na página 31.

Usando widgets

O widget contém um conjunto de ícones que permitem atualizar, alterar ou ocultar um widget.

Ícones do Widget

 Atualiza o widget, gerando os dados mais recentes.

 Abre a caixa de diálogo Configurações do Widget que permite a você gerenciar as configurações de visualização do widget. Para mais informações, consulte "Personalizando Widgets" na página 32.

Ícones do Widget (continuado)

Oculta o widget. É possível exibir o widget novamente ativando-o na área Adicionar/Remover widgets. Para mais informações, consulte "Mostrando ou Ocultando Widgets Específicos" na página 32.

NOTA Os widgets obrigatórios não possuem um ícone de fechar.

Mostrando ou Ocultando Widgets Específicos

A área **Adicionar/Remover Widgets** permite a você mostrar ou ocultar widgets opcionais específicos.

Para mostrar um widget específico:

1. Conecte-se à Central do Cliente como um Administrador ou Administrador de Segurança.
2. Na home page, na área do **Painel de controle**, clique no link **Adicionar/Remover Widgets**. O painel de controle expande e mostra uma série de caixas de seleção e botões.
3. Selecione as caixas de seleção para os aplicativos específicos que você deseja adicionar à visualização.
4. Clique em **Aplicar**. O Painel de controlo atualiza-se e mostra novos widgets.

Para ocultar widgets específicos:

1. Conecte-se à Central do Cliente como um Administrador ou Administrador de Segurança.
2. Na home page, na área do **Painel de controle**, clique no link **Adicionar/Remover Widgets**. O painel de controle expande e mostra uma série de caixas de seleção e botões.
3. Limpe as caixas de seleção para os widgets específicos que você deseja ocultar.
4. Clique em **Aplicar**. O painel de controlo se atualiza sem exibir os widgets selecionados.

Personalizando Widgets

A caixa de diálogo das Configurações de Widgets permite que você especifique várias opções de visualização para o widget selecionado.

Esta seção fornece as seguintes informações:

- Alterando as Configurações de um Widget
- Alterando as Configurações do Widget dos Relatórios Favoritos
- Deslocando a Posição de um Widget

Alterando as Configurações de um Widget

Para alterar as configurações de um widget:

1. Conecte-se à Central do Cliente como um Administrador ou Administrador de Segurança.
2. Na home page, na área do **Painel de controle**, clique no widget específico cujas configurações você deseja alterar. O diálogo das configurações de widgets para o widget específico é aberta.
3. Para alterar a aparência do widget:

a) Clique no separador de **Opções do Gráfico**. As opções para os widgets específicos são exibidas.

b) Selecione valores para as seguintes opções, conforme aplicável:

- **Tipo de Gráfico**: Selecione o tipo de gráfico dentre **Pizza**, **Barra** ou **Coluna**.
- **Paleta de Gráfico**: Selecione o esquema de cores associado ao gráfico.
- **Mostrar em 3D**: Mostrar o gráfico com efeitos tridimensionais.
- **Mostrar Porcentagem**: Para gráficos de pizza apenas, mostrar valores percentuais.

4. Para alterar o escopo dos dados apresentados em um widget:

NOTA Esta etapa só se aplica aos widgets de Taxa de Chamadas de Agente.

a) Clique no separador **Dados do Gráfico**.

b) No campo **Intervalos de Dias** digite o número de dias de dados a exibir no gráfico. Para incluir múltiplos intervalos de dias, use vírgulas para separar os valores (por exemplo, 7,14,30,60).

NOTA Para o Widget da Taxa de Chamadas (todas), por padrão, os dispositivos dormentes são excluídos do diálogo de dados do gráfico. Para incluir dispositivos dormentes, certifique-se de que marque a caixa de seleção **Incluir Dispositivos Dormentes** que está localizada na parte inferior da caixa do diálogo.

Alterando as Configurações do Widget dos Relatórios Favoritos

Para alterar as configurações do widget dos Relatórios Favoritos:

1. Conecte-se à Central do Cliente como um Administrador ou Administrador de Segurança.
2. Na home page, na área do **Painel de controle**, clique no widget dos Relatórios Favoritos.
3. No diálogo de Editar Configurações dos Relatórios Favoritos, faça qualquer uma das seguintes ações:

- Para selecionar os relatórios para serem exibidos no widget:
  i) Clique no separador **Dados dos Relatórios Favoritos**.
  ii) Na lista **Nome de Filtro**, marque a caixa de seleção adjacente ao nome do relatório preferido.
  iii) Clique em **OK** para voltar à home page da Central do Cliente com as alterações aparecendo no widget de **Relatórios Favoritos**.
- Para alterar a ordem dos relatórios exibidos no widget:
  i) Clique no separador **Dados dos Relatórios Favoritos**.
  ii) Na lista de **Nome de Filtro**, clique na linha que você deseja mover e a arraste para a posição desejada.

  Por exemplo, se você quiser que o **MeuRelatório1** seja o primeiro relatório a constar na lista no widget, então clique na linha contendo o **MeuRelatório1** e arraste a mesma para a primeira posição da lista no separador **Dados** .

  iii) Clique em **OK** para voltar à home page da Central do Cliente com as alterações aparecendo no widget de **Relatórios Favoritos**.
- Para editar o tamanho das letras:

i) Clique no separador **Opção dos Relatórios Favoritos**.
ii) Na lista **Tamanho de Fonte** selecione o valor preferido.
iii) Clique em **OK** para salvar o novo tamanho das letras e voltar à Home Page da Central do Cliente com as alterações já visíveis no widget dos **Relatórios Favoritos**.

Deslocando a Posição de um Widget

Para mover a posição do widget:

1. Conecte-se à Central do Cliente como um Administrador ou Administrador de Segurança.
2. Na Home page na área do **Painel de controle**, clique e arraste a barra do título do widget para o novo local.

Trabalhando com Seu Perfil de Usuário

Sua função de usuário e suas credenciais associadas determinam as informações que são exibidas na página Gerenciar Perfil do Usuário e aquilo que você pode acessar:

- **Administradores** e **Administradores de Segurança** podem ver e editar detalhes de usuários e todas as configurações de sistema de usuários para seus próprios perfis de usuário.

  Estas funções de usuário também podem visualizar, definir e editar as configurações da informação, do status e da suspensão de outros usuários. Consulte "Editando os Detalhes de um Usuário" na página 111.
- **Usuários de Segurança Avançados**, **Usuários Avançados** e **Usuários Convidados** podem ver e editar alguns detalhes de usuários e todas as configurações de sistema do usuário para seus próprios perfis.

Esta seção fornece as seguintes tarefas:

- Visualizando Seu Perfil de Usuário
- Editando Seu Perfil de Usuário

Visualizando Seu Perfil de Usuário

Para todas as funções de usuário da Central do Cliente, as instruções para a visualização de seu perfil de usuário são semelhantes.

Para ver seu Perfil de Usuário:

1. Conecte-se à Central do Cliente.
2. Na home page, nos links da parte superior da página e ao lado de seu Nome de Usuário, clique no link **Meu Perfil**.
3. A página Gerenciar Perfil de Usuário se abre com as seguintes seções, e sua capacidade de editar os conteúdos é dependente de sua função de usuário:
   - **Detalhes do Usuário**
   - Configurações de **Sistema do Usuário**
   - Configurações de **Status do Usuário**
   - **Configurações de auto-suspensão** (somente para as funções de usuário de Administrador e de Administrador de Segurança)

Editando Seu Perfil de Usuário

É possível acessar, ver e editar seu próprio perfil das seguintes formas:

- Editando Seus Detalhes do Usuário
- Alterando Sua Senha de Login
- Editando Suas Configurações de Sistema do Usuário
- Editando Suas Configurações de Status e Suspensão do Usuário

Editando Seus Detalhes do Usuário

NOTA Não é possível editar os campos **ID da Conta** ou **Nome de Usuário**.

Para editar seus detalhes de usuário:

1. Conecte-se à Central do Cliente.
2. Na home page, nos links da parte superior da página e ao lado de seu Nome de Usuário, clique no link **Meu Perfil**.
3. Na página Gerenciar Perfil do Usuário, na seção **Detalhes do Usuário**, faça o seguinte:
   a) No campo **E-mail**, se o valor preenchido for incorreto, digite o valor apropriado.
   b) Nos campos **Primeiro Nome** e **Sobrenome**, digite as informações apropriadas.
   c) Para ativar medidas de segurança de senhas, marque uma ou mais das seguintes caixas de seleção:
      - **O usuário deve mudar a senha no próximo login**
      - **O usuário deve mudar a senha a cada 30 dias**
      - **Exigir senha forte**

   IMPORTANTE Se sua conta de usuário requer senhas fortes, a nova senha deve conter no mínimo 8 caracteres e conter uma mistura de caracteres maiúsculos e minúsculos alfanuméricos e/ou símbolos.
4. Clique em **Salvar Alterações**.

   As alterações são salvas e a home page da Central do Cliente é aberta.

Alterando Sua Senha de Login

Para alterar a sua senha de login:

1. Conecte-se à Central do Cliente.
2. Na home page, nos links da parte superior da página e ao lado de seu Nome de Usuário, clique no link **Meu Perfil**.
3. Na página Gerenciar Perfil do Usuário, na seção **Detalhes do Usuário**, sob **Senha**, clique no link **Alterar Senha**.
4. No diálogo Alterar Senha, faça o seguinte:
   a) No campo **Inserir Senha Atual** digite sua senha existente.
   b) No campo **Definir Nova Senha** digite uma nova senha.
   c) No campo **Confirmar Nova Senha**, digite a nova senha novamente.

d) Clique em **Salvar**. O diálogo de Alterar Senha se atualiza e exibe uma mensagem confirmando as alterações que você fez.

5. Clique em **Continuar** para abrir a página Gerenciar Perfil de Usuário.
6. Clique em **Salvar Alterações** para salvar suas alterações e retornar para a página Gerenciar Perfil do Usuário.

Editando Suas Configurações de Sistema do Usuário

Para editar suas configurações de sistema do usuário:

1. Conecte-se à Central do Cliente.
2. Na home page, nos links da parte superior da página e ao lado de seu Nome de Usuário, clique no link **Meu Perfil**.
3. Na página Gerenciar Perfil do Usuário, na seção **Configurações de sistema do usuário**, faça o seguinte:

   a) No campo **Idioma e Localização do Usuário Padrão**, abra a lista e selecione as informações apropriadas.

   NOTA Se você selecionar um novo valor para o campo **Idioma e Localização do Usuário Padrão**, a data, a hora e a formatação de números são automaticamente atualizadas para refletir sua escolha.

   b) No campo **Fuso Horário Padrão**, abra a lista e selecione o fuso horário preferido.

   c) No campo **Tempo Limite Padrão da Sessão do Usuário**, abra a lista e selecione o valor desejado.

4. Clique em **Salvar Alterações**.

   As alterações são salvas e você é retornado para a home page da Central do Cliente.

Editando Suas Configurações de Status e Suspensão do Usuário

Usuários de Segurança Avançados, Usuários Avançados e Usuários Convidados podem apenas editar as configurações do **Status do Usuário** na área **Definições de status e suspensão do usuário**, enquanto Administradores e Administradores de Segurança podem editar todo o conteúdo nesta área.

Para editar suas configurações de status e suspensão do usuário:

1. Conecte-se à Central do Cliente.
2. Na home page, nos links da parte superior da página e ao lado de seu Nome de Usuário, clique no link **Meu Perfil**.
3. Na página Gerenciar Perfil do Usuário, na seção **Configurações de status e suspensão do usuário**, faça o seguinte no local apropriado:

   a) **Status do Usuário** permite que você **Suspenda** ou **Ative** usuários imediatamente; por exemplo, quando um usuário é bloqueado devido à digitação de senha incorreta por três vezes. Suas escolhas incluem:

   - **Ativo**
   - **Suspenso**

- **Temporariamente suspenso até** abre um diálogo onde você insere a data apropriada para o fim da suspensão.

b) **Auto-suspenção por login falhado** permite que administradores e administradores de segurança mitiguem tentativas propositadas de comprometer senhas, tal como a força bruta. Suas escolhas incluem:

- **Nunca auto-suspender usuário por falhas de login**
- **Auto-suspender usuário após 3 tentativas de login falhadas**
- **Auto-suspender temporariamente o usuário por 24 horas após 3 tentativas de login falhadas**

Marque a caixa de seleção para **Enviar e-mail para todos os administradores se um usuário for suspenso devido a falha de login** porque esta ação pode representar uma ameaça de segurança e você pode querer examinar quaisquer alertas associados.

c) **Auto-suspensão por inatividade** permite que administradores e administradores de segurança indiquem a suspensão apropriada para dispositivos que estão inativos e inclui as seguintes escolhas:

- **Nunca auto-suspender por inatividade**
- **Auto-suspender se o usuário não fizer login durante 30 dias**

4. Clique em **Salvar Alterações**. A Central do Cliente salva suas alterações e a sessão se reinicia novamente, retornando você para a home page.

Usando os Links Úteis

Os dois links seguintes se encontram na parte inferior da home page:

- **Suporte**: clique neste link para abrir a página de Suporte. Consulte "Contatando o Suporte Global da Absolute Software" na página 23.
- **Baixar Pacotes**: clique neste link para abrir a página Baixar Pacotes. Consulte "Baixando o Agente Computrace" na página 127.

Capítulo 3: Configurando a Central do Cliente para Seu Ambiente de Trabalho

A seção de **Administração** contém uma grande variedade de opções que você pode usar para gerenciar a Central do Cliente para as necessidades específicas de sua empresa.

Este capítulo fornece informações sobre os seguintes tópicos:

- Alertas
- Dados
- Cercas Geográficas
- Grupos de Dispositivos
- Política de Software
- Usuários
- Conta

Alertas

O recurso de alertas é usado para notificar os administradores de eventos notáveis com respeito a dispositivos gerenciados. Por exemplo, você pode querer saber se um dispositivo não conectou à rede durante um período de tempo excepcionalmente longo, potencialmente indicador de um dispositivo perdido que requer mais investigação. Neste exemplo, você poderia usar um alerta baseado na condição da Hora da Última Chamada.

Quando você configura alertas para sua empresa, um dispositivo gerenciado aciona um alerta ativo, o que depois cria um evento de alerta (isto é basicamente uma entrada em um arquivo de registro) e notifica você por e-mail ou por pager de acordo com as configurações do alerta. A mensagem de e-mail ou de pager contém um resumo das condições que acionaram o alerta e um link para a home page da Central do Cliente. Depois de uma notificação de alerta ser enviada, o alerta não se aciona novamente para esse dispositivo até o alerta ser redefinido. Você configura o alerta para ter ou uma redefinição manual ou uma redefinição automática depois de um período de tempo específico.

O recurso de Alertas é a fundação da funcionalidade de Dispositivos Suspeitos. Quando você cria um alerta, você pode atribuir um valor de nível de suspeita. Um evento de alerta único pode parecer insignificante, no entanto, quando vários eventos de alerta aparentemente insignificantes ocorrem dentro de um curto período de tempo, a atividade se torna suspeita. Quando um dispositivo aciona um ou mais alertas para quais você atribuiu valores de nível de suspeita, estes valores são consolidados e, se o resultado superar seu limite, os eventos de alerta aparecem no Relatório de Dispositivos Suspeitos (consulte "Relatório de Dispositivos Suspeitos" na página 193.). É possível usar este relatório para visualizar e gerenciar uma lista de dispositivos que têm um alto nível de atividade suspeita.

Existem dois tipos de alerta:

- **Predefinido**: A Central do Cliente vem com alertas pré-configurados (padrão) que, quando ativados, notificam você quando certos eventos ocorrem.
- **Personalizado**: É possível criar também alertas definidos pelo usuário que usam um único critério ou vários critérios. Estes alertas podem destacar ou excluir um dispositivo individual, ou grupos de dispositivos.

Os alertas possuem dois estados:

- **Ativo**: O alerta examina os dispositivos gerenciados de sua empresa para suas condições de alerta e registra os eventos de alerta quando os encontra.
- **Suspenso**: O alerta não está buscando condições de alerta e nenhuns eventos de alerta são registrados. Por padrão, todos os alertas predefinidos estão no estado Suspenso.

NOTA Os alertas por pager só podem ser recebidos por pager alfanumérico.

Esta seção fornece informações sobre os seguintes tópicos e tarefas:

- Sobre Alertas Pré-definidos
- Criando Novos Alertas Personalizados
- Criando um Alerta Baseado em Critérios de Status de Criptografia de Discos Completos
- Gerenciando Alertas
- Gerenciando Eventos de Alerta Acionados

Sobre Alertas Pré-definidos

A Central do Cliente fornece vários alertas predefinidos, que você pode ver na página Ver e Gerenciar Alertas, descrita na tarefa, "Visualizando Alertas" na página 48.

Quando os alertas predefinidos são ativados, eles executam-se como descrito na seguinte tabela. Consulte "Ativando Alertas" na página 49.

Por padrão, todos os alertas predefinidos são configurados para redefinição manual, mas você pode configurar um alerta a redefinir-se automaticamente após um número específico de dias. Consulte "Redefinindo Alertas" na página 50.

NOTA Se você tentar excluir um alerta predefinido, ele será automaticamente recriado em um estado **Suspenso**.

Alertas Pré-definidos e suas Descrições

Alertas Predefinidos (Padrão)	Descrição
Agente foi Recentemente Instalado	Este alerta é acionado quando o agente Computrace é instalado em um dispositivo. Este alerta deveria ter um tipo de redefinição de "manual" e não deveria ser redefinido a partir da página Eventos de Alerta. Fazê-lo assim resulta em alertas sendo gerados para novos dispositivos assim que se ativam, mas não no reenvio de alertas para dispositivos previamente ativados.

Alertas Pré-definidos e suas Descrições (continuado)

Alertas Predefinidos (Padrão)	Descrição
Alteração no Número de Série	Este alerta é acionado sempre que uma alteração de número de série seja detectada em um dispositivo gerenciado. Quando este alerta é configurado para se redefinir automaticamente, ele testa a condição do alerta a cada x dias, onde x é a frequência definida. **NOTA** Se um dispositivo gerenciado fizer uma chamada em que uma alteração de número de série é detectada e depois não fizer mais chamadas durante um período de tempo superior a x, é possível que o alerta se acione mais do que uma vez para o mesmo dispositivo. Quando outra chamada é realizada, no entanto, causando os dois registros de Eventos de Alerta mais recentes a não apresentar uma alteração no número de série, o alerta pára de se acionar.
Nome de Dispositivo foi Alterado	Este alerta é acionado sempre que uma alteração de nome seja detectada em um dispositivo gerenciado. É definido com um nível de Suspeita de 3.
Recompilação de Dispositivo	Este alerta é usado para proativamente notificar o administrador que um dispositivo poderá ter sido furtado. É definido com um nível de Suspeita de 3 e acionado quando *ambas* as seguintes condições são cumpridas: • Chave do produto do sistema operacional foi alterada • O dispositivo realizou uma chamada de auto-reparo
Disco Rígido Quase Cheio	Este alerta é acionado quando o espaço livre no disco rígido é inferior ou igual a 10% do total do espaço no disco rígido. Este alerta coincide com os resultados no relatório do espaço disponível em disco rígido na Central do Cliente, se aquele relatório usar o mesmo grupo de dispositivos e definição de 10%. Se este alerta for configurado a redefinir-se automaticamente, ele testa esta condição a cada x dias e aciona-se nos mesmos dispositivos cada vez até que o espaço no disco rígido seja limpo e tenha mais de 10% disponível.
Última Chamada há 20 dias	O acionador para este alerta é a condição de **Hora da Última Chamada**. Se estiver configurado para se redefinir automaticamente, este alerta testa a condição a cada x dias e se aciona no mesmo dispositivo cada vez até que realizem outra chamada. Em outras palavras, quando o dispositivo fizer uma chamada, o alerta já não se aciona para aquele dispositivo. É uma prática recomendada configurar este alerta para se redefinir automaticamente para manter o controle sobre seus dispositivos que falham em realizar chamadas, mesmo que esta configuração resulte em um grande número de notificações enviadas por e-mail.

Alertas Pré-definidos e suas Descrições (continuado)

Alertas Predefinidos (Padrão)	Descrição
Terminação da concessão	Este alerta compara a data na condição da **Data de Fim da Concessão** às definições configuradas para o alerta. Quando a **Data de Fim da Concessão** for menos ou igual a 14 dias da data atual, a configuração padrão aciona um alerta que envia uma mensagem de e-mail com uma lista de todos os dispositivos que atendem aos critérios. Se este alerta está configurado para se redefinir automaticamente, ele reenvia o alerta a cada x dias, onde x é a frequência definida nas configurações de alerta. Este alerta continua a se acionar depois da **Data de fim da Concessão** já ter passado até você redefini-lo.
Endereço IP local alterado	Este alerta é acionado sempre que uma alteração de endereço IP local seja detectada em um dispositivo gerenciado. É definido com um nível de Suspeita de 1.
Alteração Significativa	Este alerta é usado para proativamente notificar o administrador que um dispositivo poderá ter sido furtado. É definido com um nível de Suspeita de 5 e acionado quando *todas* as seguintes condições são cumpridas: ● Chave do produto do sistema operacional foi alterada ● Nome do dispositivo foi alterado ● Nome de usuário foi alterado ● O dispositivo realizou uma chamada de auto-reparo
Software em falta na lista de obrigatórios	Este alerta é acionado pela não conformidade com uma política de software. Um alerta de Software em falta em uma lista de Obrigatórios aciona o alerta para qualquer dispositivo gerenciado em que é detectado que um pacote de software obrigatório não está instalado. Se este alerta estiver configurado para se redefinir automaticamente, ele é acionado nos mesmos dispositivos todos os dias até que a ação corretiva seja tomada e o dispositivo não viola mais esta política.
Modem foi alterado	Este alerta é acionado sempre que exista uma alteração no status do modem entre a penúltima e a última chamada feita para um dispositivo gerenciado específico. Este alerta não indica a data da penúltima chamada, no entanto, é possível consultá-la no Relatório do Histórico de Chamadas. Visto que este alerta compara as duas últimas datas de chamada para um dispositivo gerenciado em particular, a redefinição do alerta pode resultar na geração do alerta mais de uma vez para um único dispositivo.
Rede foi alterada	Este alerta é acionado quando tanto o endereço IP local e o endereço IP público são alterados em um dispositivo, o que pode indicar que o dispositivo já não está ligado à rede. É definido com um nível de Suspeita de 2.

Alertas Pré-definidos e suas Descrições (continuado)

Alertas Predefinidos (Padrão)	Descrição
Novo Arquivo de Programa Detectado	Tanto aplicativos novos como atualizados acionam este alerta. Independentemente do número de novos aplicativos instalados em um dispositivo gerenciado específico, este alerta se aciona uma vez e não se aciona novamente até você o redefinir. Se o alerta estiver configurado para se redefinir automaticamente, ele testa a condição do alerta a cada x dias, onde x é a frequência definida. Visto que a condição se baseia na comparação da data detectada de software com a data de modificação de alerta, ela aciona um alerta nos mesmos aplicativos a cada x dias, a não ser que o alerta em si é modificado e salvo, alterando assim a data de modificação do alerta. No entanto, se o alerta estiver configurado para se redefinir manualmente, ele só se aciona uma vez em um dispositivo gerenciado específico, até que este seja reiniciado, mesmo que o novo aplicativo seja instalado subsequentemente.
Sistema operacional alterado	Este alerta é acionado sempre que uma alteração de sistema operacional seja detectada em um dispositivo. Isto pode se dever a novas gerações de imagens implantadas no dispositivo, mas também poderá indicar que o dispositivo foi furtado. É definido com um nível de Suspeita de 2.
Chave do produto do sistema operacional alterada	Este alerta é acionado sempre que uma alteração de chave do produto do sistema operacional seja detectada em um dispositivo, o que pode indicar que o dispositivo foi furtado e que o ladrão pode ter formatado o dispositivo. É definido com um nível de Suspeita de 3.
Endereço de IP público alterado	Este alerta é acionado sempre que uma alteração de endereço IP local seja detectada em um dispositivo gerenciado. É definido com um nível de Suspeita de 1.
Chamada de auto-reparo	Este alerta é acionado sempre que um dispositivo fizer uma chamada de auto-reparo. É usado para notificar um administrador que o agente em um dispositivo foi violado ou removido do dispositivo. O agente podia ter sido temporariamente removido durante um processo de TI normal, mas isto também poderia sinalizar uma tentativa maliciosa de remover o agente do dispositivo. É definido com um nível de Suspeita de 3.
Software na Lista de Proibidos	Este alerta é acionado pela não conformidade com uma política de software. Software que está definido como proibido aciona um alerta se for detectado em qualquer dispositivo. Se este alerta estiver configurado para se redefinir automaticamente, ele é acionado nos mesmos dispositivos todos os dias até que a ação corretiva seja tomada para garantir que o dispositivo não viole mais esta política.

Alertas Pré-definidos e suas Descrições (continuado)

Alertas Predefinidos (Padrão)	Descrição
Nome de usuário alterado	Este alerta é acionado sempre que uma alteração de nome de usuário seja detectada em um dispositivo, o que pode indicar que o dispositivo está sendo usado por outro usuário e que podia ter sido furtado. É definido com um nível de Suspeita de 3.
Garantia está terminando	Este alerta compara a data no campo **Data de Fim da Garantia** às definições configuradas para o alerta. A configuração padrão aciona o alerta quando a **Data de Fim da Garantia** for menor ou igual a 14 dias até a data atual. Quando acionado, este alerta envia uma notificação por e-mail que inclui uma lista de todos os dispositivos que atendem aos critérios. Se este alerta está configurado para se redefinir automaticamente, ele reenvia o alerta a cada x dias, onde x é a frequência definida nas configurações de alerta. Este alerta continua a se acionar depois da **Data de fim da Garantia** já ter passado até você redefini-lo.

Criando Novos Alertas Personalizados

É possível criar alertas que atendem às necessidades específicas de sua empresa.

Para criar um novo alerta personalizado:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Alertas**>**Criar e Editar Alertas**.
3. Na página Criar e Editar Alertas, no campo **Nome de Alerta**, digite um nome apropriado para o alerta. Este nome aparece na coluna **Nome de Alerta** na grelha de resultados da página Eventos de Alerta.
4. No campo **Descrição do Alerta**, digite uma descrição apropriada para este alerta.
5. No campo **Nível de Suspeita**, abra a lista e selecione um nível de severidade para eventos suspeitos. Possíveis valores variam desde **Não é Suspeito** até um nível de suspeição de**5**.

   Este valor é exibido no Relatório de Dispositivos Suspeitos, que realça os dispositivos com atividades suspeitas. Consulte "Relatório de Dispositivos Suspeitos" na página 193.

   NOTA Ao definir níveis de suspeita, você precisa considerar as implicações do alerta. Por exemplo, uma concessão terminando é comportamento esperado, enquanto a substituição de um disco rígido pode indicar um dispositivo furtado.

6. Na área **Condições**, defina as condições que acionam o alerta.

   Um único alerta pode ter várias condições separadas que devem ser todas atendidas para acionar a notificação do usuário.

   IMPORTANTE Condições prefixadas com um asterisco (*) não são acionadas pelas chamadas de agente e só podem ser combinadas com outras condições que têm um asterisco.

a) Abra a lista **Campo** e selecione o valor desejado.
b) Abra a lista **Regras** e selecione o valor desejado. Esta lista inclui todas as regras aplicáveis para o campo selecionado na lista de **Campo**.
c) Dependendo das suas seleções nas listas **Campo** e **Regra**, o campo **Critérios** poderá abrir.
Faça uma das seguintes ações para fornecer informações para o campo **Critérios**:
   - Digite o valor apropriado.
   - Clique em **Escolher** para abrir um diálogo que fornece uma lista de todos os critérios existentes. Clique no valor desejado na lista. O diálogo se fecha e atualiza a página Criar e Editar Alertas, preenchendo o campo de **critérios** com sua seleção.

d) Clique em **Adicionar Condição**. A página é atualizada e mostra a nova condição na tabela de **Condições**.
Repita esta etapa até todas as condições apropriadas serem adicionadas.

NOTA Para excluir uma condição existente de um alerta, clique em **Excluir**.

7. Na área **Escopo**, indique quais os grupos de dispositivos que atendem aos critérios especificados e que estão incluídos no ou excluídos do alerta que você está criando.
   - Na área **Inclui**, selecione os dispositivos que você deseja incluir no relatório da seguinte forma:
     - Abra a lista **Dispositivos no grupo** e selecione o grupo de dispositivos a que se aplica este alerta.

       NOTA Se um ou mais dispositivos em seu grupo de dispositivos selecionado foram relatados como furtados, o alerta não se aplica a estes dispositivos.

     - Abra a lista **Apenas onde o** e selecione o valor desejado. Os valores incluem **Quaisquer dos campos nesta lista**, **Identificador**, **Nome de Dispositivo**, **Nome de Usuário** e **Número de Série**.
     - No campo **é ou contém** digite os critérios de pesquisa. É possível também usar **Escolher** para selecionar um valor da lista de todos os critérios existentes.
   - Na área **Exclui**, selecione os dispositivos que você deseja excluir do relatório:
     - Abra a lista **Dispositivos no grupo** e selecione o grupo de dispositivos a que não se aplica este alerta.
     - Abra a lista **Apenas onde o** e selecione o valor desejado. Os valores incluem **Quaisquer dos campos nesta lista**, **Identificador**, **Nome de Dispositivo**, **Nome de Usuário** e **Número de Série**.
     - No campo **é ou contém** digite os critérios de pesquisa. É possível também usar **Escolher** para selecionar um valor da lista de todos os critérios existentes.
8. Quando um dispositivo aciona um alerta, o mesmo dispositivo não pode acionar o alerta novamente até o evento de alerta ser redefinido para o dispositivo individual ou para todos os dispositivos. Dispositivos relatados como furtados não acionam um alerta.

   Na área **Tipo de Alerta** defina como o alerta será redefinido para o dispositivo que o acionou:
   - Para criar um alerta que você precisa redefinir manualmente a partir da página Eventos de Alerta, selecione a opção **Redefinição manual**.

- Para criar um alerta que se redefine automaticamente após um certo número de dias, selecione a opção **Redefinir automaticamente após**e depois digite um valor no campo **dia (s)**.

9. Na área **Opção de Alerta**, especifique se é para enviar um único alerta por email ou vários alertas por emails quando o alerta for acionado por vários dispositivos.
   - Para enviar uma única mensagem de e-mail consolidada que fornece detalhes sobre cada dispositivo que acionou o alerta, selecione a opção **E-mail individual**
   - Para enviar um e-mail individual a partir de cada dispositivo que aciona o alerta, selecione a opção **Múltiplos e-mails**, o que pode resultar em um grande número de e-mails.
10. Na área **Ação** defina como a Central do Cliente deve tratar o alerta quando o mesmo for acionado.

    A Central do Cliente registra sempre alertas acionados para o relatório de Dispositivos Suspeitos. Por padrão, a Central do Cliente também notifica os administradores por email ou pager quando um alerta é acionado.

    É possível definir um alerta de forma que nenhuma notificação seja enviada; por exemplo, ao criar um alerta considerado de baixo nível.
   - Para não enviar nenhuma notificação quando o alerta for acionado, selecione **Registrar evento**.
   - Para contatar administradores automaticamente usando mensagens de e-mail ou de pager quando o alerta é acionado, selecione **Registrar o evento e notificar**.
   - Para enviar notificações de alerta por e-mail, digite um ou mais endereços no campo **Endereço de e-mail**. Separe múltiplos endereços de e-mail com um ponto-e-vírgula.
   - Para enviar notificações de alerta para um pageralfa-numérico, no campo **Pager** digite o endereço do pager de destino. É possível inserir múltiplos destinatários ao separar os endereços com um ponto-e-vírgula.
11. Se você não quiser ativar o alerta nesta altura, selecione a opção **Suspender verificação de alertas**.
12. Clique em **Salvar**.

    Você é retornado à página de onde tinha navegado para a página Criar e Editar Alertas e uma mensagem de confirmação é mostrado a você nessa página.

Exemplos de Condições de Alerta

Os seguintes exemplos descrevem algumas condições comumente usadas para os alertas:

- Criando um Alerta de Cerca Geográfica
- Criando um Alerta Baseado em Critérios de Status de Criptografia de Discos Completos

Criando um Alerta de Cerca Geográfica

Para definir uma condição de alerta para acionar um alerta quando um dispositivo se deslocar para fora da localização da cerca geográfica:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Alertas**>**Criar e Editar Alertas**.

3. Na página Criar e Editar Alertas, na área **Condição**, abra a lista **Campo** e selecione o valor **Localização de Cerca Geográfica**.
4. A **área de Condição** atualiza-se. Complete as seguintes etapas:
   a) Abra a lista **Regras** e selecione uma das seguintes opções:
      - **Está dentro**: cria um alerta sempre que um dispositivo se desloca dentro de um limite de Cerca Geográfica especificado.
      - **Está fora**: cria um alerta sempre que um dispositivo se desloca para fora do limite da cerca geográfica.

   b) O campo adjacente ao campo de **Regras** contém a lista de cercas geográficas que existem para sua conta. Abra a lista e selecione o nome da Cerca Geográfica desejado.

   c) Os restantes campos permitem que você especifique o período de tempo após qual o alerta é acionado. Insira o número apropriado no campo **por pelo menos** e selecione **Horas**, **Dias** ou **Semanas** para especificar a unidade de tempo.
5. Clique em **Adicionar condição**.
6. Insira o resto das informações que sejam apropriadas para este alerta de Cerca Geográfica, como descrito na etapa 7 a etapa 12 da tarefa, "Criando Novos Alertas Personalizados" na página 43.

Criando um Alerta Baseado em Critérios de Status de Criptografia de Discos Completos

É possível criar alertas baseados em cadeias de status de criptografia e condições definidas na área de filtragem do Relatório do Status de Criptografia de Discos Completos. Para mais informações sobre este tipo de relatório, consulte "Relatório do Status de Criptografia de Discos Completos" na página 197. Por exemplo, você pode querer receber um alerta sempre que a cadeia do Status de Criptografia se altere.

IMPORTANTE Atualmente, o Relatório do Status de Criptografia de Discos Completos fornece somente informações sobre produtos de criptografia de discos completos instalados no sistema ou na primeira unidade física apenas.

Para criar um alerta de criptografia:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Segurança** > **Relatório do Status de Criptografia de Discos Completos**.
3. Na página Relatório do Status de Criptografia de Discos Completos, na área **e onde a cadeia do Status de Criptografia**, defina a filtragem preferida para o relatório. Para mais informações, consulte "Filtrando Dados para Criar um Relatório do Status de Criptografia de Discos Completos" na página 200.
4. Clique no link **Criar um alerta baseado neste critério de status de criptografia**.
5. Um diálogo de aviso se abre indicando que quaisquer critérios de pesquisa não salvos serão perdidos caso você proceda. Para continuar, clique em **OK**.
6. Na página Criar e Editar Alertas, no campo **Nome de Alerta**, digite um nome apropriado para este alerta.
7. No campo **Descrição do Alerta**, digite uma descrição apropriada para este alerta de criptografia.

8. Abra a lista **Nível de Suspeita** e selecione o nível apropriado como descrito na etapa 3 da tarefa, "Criando Novos Alertas Personalizados" na página 43.

9. A tabela **Condições** inclui as opções que você forneceu quando filtrou os dados no Relatório do Status de Criptografia de Discos Completos. Consulte "Filtrando Dados para Criar um Relatório do Status de Criptografia de Discos Completos" na página 200.

   Se for necessário, você poderá definir mais condições para acionar um alerta de criptografia da seguinte maneira:

   a) Abra a lista **Regras** e escolha a partir das seguintes opções, se aplicável:
      - **Começa com**
      - **Foi alterado**
      - **Contém**
      - **Não começa com**
      - **Não contém**
      - **É**
      - **Não é**

   b) Dependendo das suas seleções nas listas **CampoeRegras**, o campo **Critérios** pode abrir. Clique em **Escolher** para abrir o diálogo de Escolher e selecionar a entrada apropriada da lista.

      Apenas aqueles produtos detectados para sua conta aparecem no diálogo Escolher. Selecione o produto apropriado, que será adicionado às suas condições automaticamente.

   c) Clique em **Adicionar condição**.

      A página é atualizada e mostra a nova condição ou novas condições que você definiu para este alerta na tabela de **Condição**.

      NOTA Para excluir uma condição existente de um alerta, clique em **Excluir**.

10. Insira o resto das informações que sejam apropriadas para este alerta de criptografia, como descrito na etapa 7 a etapa 12 da tarefa, "Criando Novos Alertas Personalizados" na página 43.

Se você parar a criptografia de discos completos, quando você voltar a ligar este recurso irá necessitar reativar quaisquer alertas de criptografia que você criou. Para mais informações, consulte "Reativando Alertas Suspensos" na página 49.

Gerenciando Alertas

Gerencia-se alertas predefinidos e personalizados da mesma forma, e você pode realizar as seguintes tarefas em ambos os tipos de alertas:

- Visualizando Alertas
- Pesquisando um Alerta Específico
- Ativando Alertas
- Editando Alertas
- Reativando Alertas Suspensos
- Redefinindo Alertas
- Suspendendo Alertas
- Excluindo Alertas

Visualizando Alertas

A página Visualizar e Gerenciar Alertas exibe uma tabela com um registro para todos os alertas existentes, incluindo os atributos e status para cada alerta.

NOTA É possível aplicar um alerta a um dispositivo individual ou a um grupo de dispositivos, enquanto *eventos de alerta* se referem sempre a um dispositivo individual.

Para visualizar os alertas existentes:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Alertas** > **Ver e Gerenciar Alertas**.
3. Na página Ver e Gerenciar Alertas, por padrão a grelha de resultados mostra todos os alertas existentes, organizados nas seguintes colunas:
   - **ID do Alerta** fornece o número que é gerado pela Central do Cliente.
   - **Nome do Alerta** é o nome deste alerta.
   - **Condições** mostra as condições que foram definidas para este alerta.
   - **Inclusão de Escopo** indica o critério específico para os dispositivos que acionam alertas.
   - **Exclusão de Escopo** indica os critérios especificados para os dispositivos que foram excluídos deste alerta.
   - **Nível de Suspeita** é o nível de suspeita definido para este alerta. Se nenhum valor existir um nível de suspeita não foi definido.
   - **Status** mostra o status atual do dispositivo.
   - **Tipo** indica como o alerta é redefinido depois do mesmo ser acionado, tal como redefinição **Manual** ou **Automática**.

Pesquisando um Alerta Específico

É possível usar a opção Critérios de Pesquisa para localizar um alerta específico.

Para pesquisar um alerta específico:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Alertas** > **Ver e Gerenciar Alertas**.
3. Na página Ver e Gerenciar Alertas, você pode pesquisar da seguinte forma:
   - Na área **Critérios de Pesquisa** abra a lista **a ID do Alerta é** e selecione o número da ID desejado.
   - No campo **e o Nome do Alerta contém**, digite todo ou parte do nome do alertar que você deseja localizar.
   - Adjacente a **e o nível de suspeita é**:
     i) Abra a primeira lista e selecione uma das seguintes opções:
        – **>** maior que
        – **>=** maior que ou igual a
        – **=** igual a
        – **<=** menor que ou igual a
        – **<** menor que

ii) Abra a segunda lista e selecione um valor de **0** a **5**.

4. Clique em **Mostrar Resultados** para gerar novamente o relatório usando os critérios definidos.

Ativando Alertas

Alertas predefinidos e personalizados aparecem no estado **Suspenso** até você os ativar.

Para ativar um alerta:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Alertas** > **Ver e Gerenciar Alertas**.
3. Na página Ver e Gerenciar Alertas, a lista de alertas aparece na grelha de resultados. Escolha os alertas que você deseja ativar de uma das seguintes formas:
   - Para ativar um ou mais alertas, faça uma revisão à lista de alertas e marque a caixa de seleção para cada alerta que você deseja ativar.
   - Para ativar todos os alertas, marque a caixa de seleção na linha de cabeçalho **ID do Alerta**. Todas as caixas de seleção nessa coluna estão agora marcadas
4. Clique em **Ativar**.

   Na grelha de resultados o **Status** para os alertas selecionados é agora **Ativo**.

Editando Alertas

É possível editar tanto alertas predefinidos como personalizados.

Para editar um alerta:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Alertas** > **Ver e Gerenciar Alertas**.
3. Na página Ver e Gerenciar Alertas, na grelha de resultados, clique em **ID de Alerta** para o alerta que você deseja editar.
4. Na página Criar e Editar Alertas, edite os valores tal como descrito na etapa 3 a etapa 12 da tarefa, "Criando Novos Alertas Personalizados" na página 43.

Reativando Alertas Suspensos

É possível reativar alertas que suspendeu; por exemplo, alertas de criptografia se você decidiu desligar a criptografia de discos completos para um grupo de dispositivos.

Para reativar alertas suspensos:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Alertas** > **Ver e Gerenciar Alertas**.
3. Na página Ver e Gerenciar Alertas, na grelha de resultados, localize o alerta **Suspenso** que você deseja reativar e marque sua caixa de seleção.
4. Clique em **Ativar**.

Redefinindo Alertas

É possível configurar um alerta para se redefinir automaticamente ou sob demanda (manualmente) depois do alerta ser acionado por um dispositivo. O dispositivo não acionará o alerta novamente até ele ser redefinido. Outros dispositivos ainda acionarão este alerta.

Para redefinir um alerta:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, siga um destes procedimentos:
   - Para redefinir um alerta em todos os dispositivos em que o alerta foi acionado:
     i) Clique **Administração** > **Alertas** > **Ver e Gerenciar Alertas**.
     ii) Na página Ver e Gerenciar Alertas marque a caixa de seleção para alerta **Ativo** que você deseja redefinir. Não é possível redefinir um alerta **Suspenso**.
     iii) Clique em**Redefinir**.

     O alerta é redefinido em todos os dispositivos em que foi acionado.
   - Para redefinir um alerta em dispositivos individuais:
     i) Clique **Administração** > **Alertas** > **Eventos de Alerta**.
     i) Na página Eventos de alerta marque a caixa de seleção para o alerta que você deseja redefinir. É possível selecionar vários alertas.
     ii) Clique em**Redefinir**.

     O alerta é redefinido em cada dispositivo associado, assim como indicado na coluna Identificador. A data e hora atuais aparecem na coluna **Data de Redefinição**.

NOTA Se as condições que inicialmente acionaram o alerta permanecerem, o alerta será acionado novamente e as mensagens de notificação voltarão a ser enviadas.

Suspendendo Alertas

Pode haver alturas quando você deseja suspender alertas. Por exemplo, se você representa um distrito escolar e recebe atualmente alertas de seus dispositivos gerenciados quando estes não fazem chamadas a cada três semanas, você pode querer suspender este alerta durante as férias de verão.

Para suspender um alerta:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Alertas**.
3. É possível suspender alertas de uma destas maneiras:
   - Para criar um alerta personalizado no estado **Suspenso**:
     i) Clique no link **Criar e Editar Alertas**.
     ii) Siga as instruções fornecidas na tarefa, "Criando Novos Alertas Personalizados" na página 43.
     iii) Na parte inferior da página, marque a caixa de seleção **Suspender a verificação de alertas**.
     iv) Clique em **Salvar**. A Central do Cliente não verifica este alerta até você o ativar.
   - Para suspender um ou mais alertas:
     i) Clique no link **Ver e Gerenciar Alertas**.

ii) Na grelha de resultados selecione os alertas que você deseja suspender de uma das seguintes formas:
   - Para suspender um ou mais alertas, faça uma revisão à lista de alertas e marque a caixa de seleção para cada alerta que você deseja suspender.
   - Para suspender todos os alertas, marque a caixa de seleção na fila do cabeçalho da coluna ajdacente a**lD do Alerta**. Todas as caixas de seleção estarão agora marcadas.

iii) Clique em **Suspender**. Na grelha de resultados o **Status** para os alertas selecionados é agora **Suspenso**.

Excluindo Alertas

É possível excluir alertas que você, ou outros usuários, têm criado. No entanto, se você tentar excluir um alerta predefinido, ele será recriado em um estado **Suspenso**.

Para excluir um alerta:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Alertas** > **Ver e Gerenciar Alertas**.
3. Na página Ver e Gerenciar Alertas, na grelha de resultados, localize o alerta que você deseja excluir e depois faça uma das seguintes ações:
   - Marque a caixa de seleção para o alerta e clique em **Excluir**.
   - Clique no link na coluna **ID de Alerta** e na página Criar e Editar Alertas, clique **Excluir**.
4. Um diálogo de aviso se abre indicando que se você excluir este alerta, também exclui todos os registros (tais como eventos de alerta) associados a ele.

   Clique em**Continuar** para excluir este alerta.

   NOTA Se o alerta que você excluiu era um alerta predefinido, seu status será atualizado para **Suspenso** e aparecerá na parte inferior da grelha de resultados com um novo **ID de Alerta**.

Gerenciando Eventos de Alerta Acionados

A página Eventos de Alerta mostra uma tabela (grelha de resultados) que contém registros dos alertas que foram acionados para cada dispositivo.

Esta seção fornece as seguintes informações e tarefas:

- Visualizando Eventos de Alerta Acionados
- Baixando Eventos de Alerta

Visualizando Eventos de Alerta Acionados

A página Eventos de Alerta mostra uma tabela (grelha de resultados) que contém registros dos alertas que foram acionados para cada dispositivo.

NOTA Por padrão, sete dias de informações aparecem na grelha de resultados. É possível alterar o que aparece, baseado nas datas definidas na área **e o Evento ocorreu**.

Para filtrar e ver eventos de alerta:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Alertas > Eventos de Alerta**.
3. Na página Eventos de Alerta, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por um evento de alerta específico, faça o seguinte:
     i) Abra a lista **o campo** e selecione um dos seguintes valores:
        - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique em um identificador na grelha de resultados para abrir a página Resumo do Dispositivo desse dispositivo.
        - **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
        - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
        - **ID do Alerta**: o número atribúido a este alerta pela Central do Cliente.
        - **Nome do Alerta**: o nome do alerta.

     ii) No campo **é ou contém** digite um valor.
   - Para filtrar seus resultados pelo nível de suspeita, faça o seguinte:
     i) Abra a lista adjacente a **e o Nível de Suspeita** e selecione uma das seguintes opções:
        - **<** para um valor que é menor que
        - **<=** para um valor que é menor que ou igual a
        - **=** para um valor que iguala
        - **>=** para um valor que é maior que ou igual a
        - **>** para um valor que é maior que

     ii) Abra a segunda lista e selecione um valor de **0** a **5**.
   - Para filtrar seus resultados pela data quando o evento de alerta foi acionado, na área **e o Evento ocorreu**, faça uma das seguintes opções:
     - Clique na opção **nos últimos <n> dias** e digite o número de dias desejado no campo. Valores de **1** a **365** são suportados Um valor superior neste campo resulta em um relatório maior que demora mais tempo a ser gerado.
     - Clique na opção **entre** e digite as datas de início e de fim (dd/mm/aaaa). Alternativamente, clique no ícone do **Calendário** ao lado de cada campo de data para abrir o diálogo do calendário. Insira a data de início no campo de primeira data e a data final no segundo.
4. Clique em **Mostrar Resultados**. A grelha de resultados é atualizada e mostra a lista de alertas que foram acionados e que tiveram notificações enviadas por e-mail. Os seguintes dados são retornados de acordo com as suas escolhas de filtragem:
   - **ID do Alerta** é o número atribuído a este alerta pela Central do Cliente.
   - **Nome do Alerta** é o nome deste alerta.
   - **Identificador** é o identificador único (número de série eletrônico) para este dispositivo.
   - **Nome de Usuário** é o usuário que estava conectado ao dispositivo.
   - **Nome de Dispositivo** é o nome deste dispositivo.

- **Data de Redefinição** indica a data em que este alerta foi redefinido para que possa continuar a acionar o alerta.
- **Último Evento** indica a data e a hora do último evento de alerta deste dispositivo.
- **Nível de Suspeita** é o nível de suspeita definido para este alerta. Se esta célula estiver vazio significa que nenhum nível de suspeita foi definido.
- **Status** indica se o alerta está **Ativo** ou **Suspenso**.

Baixando Eventos de Alerta

A página Eventos de Alerta mostra uma tabela (grelha de resultados) que contém registros dos alertas que foram acionados para cada dispositivo.

NOTA Por padrão, sete dias de informações aparecem na grelha de resultados. É possível alterar o que aparece, baseado nas datas definidas na área **e o Evento ocorreu**.

Para baixar eventos de alerta:

1. Complete a tarefa, "Visualizando Eventos de Alerta Acionados" na página 51.
2. Na grelha de resultados, selecione os alertas que você deseja baixar ao fazer uma das seguintes ações:
   - Para selecionar um ou mais eventos de alerta, faça uma revisão à lista de eventos de alerta e marque a caixa de seleção para cada alerta que você deseja baixar.
   - Para selecionar todos os eventos de alerta, marque a caixa de seleção na linha de cabeçalho da coluna ajdacente a**ID do Alerta**. Todas as caixas de seleção nessa coluna estão agora marcadas.
3. Na parte superior da grelha de resultados clique em .
4. Na página Relatório de Solicitação: Eventos de Alerta, no campo **Nome de Relatório**, digite um nome para este relatório que você deseja baixar.
5. Abra a lista **Formato de Relatório**e selecione um formato de arquivo.
6. Na área de **Criar Alerta de E-mail**, se você deseja receber uma notificação por e-mail quando o arquivo estiver disponível, insira seu endereço de e-mail no campo **Seu Endereço de E-mail**.
7. Clique em**Continuar**.

Você receberá um email quando seu relatório for gerado. É possível recuperar o arquivo do relatório na página Meus Relatórios. Para informações sobre a recuperação de relatórios, consulte "Baixando Relatórios" na página 150.

Dados

O agente Computrace recolhe informações diretamente de cada dispositivo gerenciado. É possível também adicionar dados empresariais pertencentes a cada dispositivo usando a página Dados da Central do Cliente. Estas informações adicionais estão depois disponíveis em uma seleção de relatórios, tais como o relatórios de **Ativos** e de **Conclusão de Concessão**.

Esta seção fornece informações sobre os seguintes tópicos:

- Usando Departamentos
- Exportando e Importando Dados

- Visualizando e Editando Campos de Dados
- Migrando Dados Entre Dispositivos
- Gerenciando Definições de Campos Fixos e Definidos pelo Usuário
- Usando Mensagens do Usuário Final

Usando Departamentos

É possível inserir os departamentos de sua empresa na Central do Cliente para poder lhes atribuir dispositivos e depois filtrar os relatórios de dispositivos por departamento.

Os administradores podem permitir ou limitar a visibilidade de departamentos a nível de usuário.

Esta seção descreve as seguintes tarefas:

- Visualizando um Departamento
- Criando um Departamento
- Editando um Departamento
- Adicionando Dispositivos a um Departamento
- Visualizando os Dispositivos em um Departamento
- Removendo Dispositivos de um Departamento
- Excluindo um Departamento

Visualizando um Departamento

Para visualizar um departamento:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Dados** > **Criar e Editar Departamentos**.

   Na página Criar e Editar Departamentos, a grelha de resultados mostra a lista de departamentos associados à sua conta. Os valores na coluna **Contagem de Identificadores** indica o número de dispositivos em cada departamento.

Criando um Departamento

Para criar um departamento:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.
2. No painel de navegação, clique **Administração** > **Dados** > **Criar e Editar Departamentos**.
3. Na página Criar e Editar Departamentos , clique**Criar Novo Departamento**.
4. No campo **Nome de Departamento**, digite um nome apropriado.
5. Clique em **Salvar**.

   A página Criar e Editar Departamento se atualiza com uma mensagem confirmando que o novo departamento foi salvo.

   O novo nome de departamento aparece na grelha de resultados e inclui uma **Contagem de Identificadores** e uma link de**Editar**.

Editando um Departamento

Para editar o nome de um departamento:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.
2. No painel de navegação, clique **Administração** > **Dados** > **Criar e Editar Departamentos**.
3. Na página Criar e Editar Departamentos, na grelha de resultados, clique no link **Editar** para o departamento que você deseja editar.
4. No campo **Nome de Departamento**, edite o nome do departamento.
5. Clique em **Salvar**.

   A página Criar e Editar Departamentos se atualiza e mostra uma mensagem que confirma que suas alterações foram salvas.

Adicionando Dispositivos a um Departamento

A Central do Cliente armazena a atribuição de departamentos de um dispositivo como um campo de dados. Para adicionar um dispositivo só a um departamento, consulte "Atribuindo Valores de Dados a Um Dispositivo Individual" na página 60. Para adicionar um grupo de dispositivos a um departamento, consulte "Atribuindo Valores de Dados a Todos os Dispositivos em um Grupo de Dispositivos" na página 60.

Visualizando os Dispositivos em um Departamento

Para ver que dispositivos estão em que departamentos usando o relatório de ativos:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Hardware** > **Relatório de Ativos**.
3. Na página Relatório de Ativos, no local de Critérios de Pesquisa, sob a área **Mostrar todos os Dispositivos onde**, filtre os dados para mostrar todos os dispositivos associados a este departamento.

   a) No campo **e o Grupo é**, abra a lista e selecione **Todos os Dispositivos**.

   b) Abra a lista **e o campo** e selecione o campo desejado para limitar sua pesquisa.

   c) Faça uma das seguintes opções:

   - No campo **é ou contém**, digite o valor desejado para o campo que você selecionou.
   - Clique em**Escolher**.

     No diálogo Escolher, faça uma das seguintes ações:

     - Digite o valor apropriado no campo e clique em **Filtrar**.
     - Na tabela, clique no **Identificador** apropriado para o selecionar.

     O diálogo de Escolher se fecha e o campo no Relatório de Ativos é preenchido com sua seleção.

   d) Abra a lista **e quando** e selecione **Chamada mais recente**.

   e) Selecione a opção apropriada a partir do seguinte:

   - Clique na opção de **a qualquer hora**, se isto for apropriado.
   - Clique na opção **nos últimos <n> dias** e digite o número de dias desejado para sua pesquisa, de **1** a **365**.

- Clique na opção **entre** e digite as datas de início e de fim (dd/mm/aaaa). Alternativamente, clique no ícone do **Calendário** ao lado de cada campo de data para abrir o diálogo do calendário. Insira a data de início no campo de primeira data e a data final no segundo.

f) Na área **e o Agente**, se certifique de que **Qualquer Tipo** aparece no campo **tipo** e que **Qualquer Versão** aparece no campo**e versão**.

g) Abra a lista **e o Departamento é** e selecione o departamento que você deseja ver.

h) Abra a lista **e o Status do Agente é** e selecione **Todos**.

i) Na área **Mostrar resultados**, marque as caixas de seleção de **Com campos definidos pelo usuário** e **Incluir Dispositivos Inativos**.

Os administradores podem atribuir o status **Dispositivo Inativo** àqueles dispositivos que não fazem chamadas para o Centro de Monitoramento regularmente.

4. Clique **Mostrar Resultados** para atualizar a grelha de resultados.
5. Para baixar, imprimir ou salvar este relatório você tem as seguintes opções:

- Para baixar o relatório, clique . O Relatório de Solicitação: A página Relatório de Ativos se abre e você faz o seguinte:
  i) No campo **Nome de Relatório**, digite um nome para este relatório que você deseja baixar.
  ii) Abra a lista **Formato de Relatório**e selecione **CSV** se você pretende editar o relatório e carregá-lo.
  iii) Na área de **Criar Alerta de E-mail**, se você deseja receber uma notificação por e-mail quando o arquivo estiver disponível, insira seu endereço de e-mail no campo **Seu Endereço de E-mail**.
  iv) Clique em**Continuar**.

- Para imprimir a página atual do relatório, clique em e siga as solicitações da tela. Dependendo de seu sistema operacional, você pode **Abrir**, **Salvar**, **Salvar Como**, **Salvar e abrir**, ou **Cancelar** esta solicitação.

- Para salvar os filtros usados para este relatório, clique em e no diálogo Salvar Filtro de Relatório, digite um nome para o filtro e clique em **OK**.

Removendo Dispositivos de um Departamento

É possível remover dispositivos de um departamento ao remover os valores de dados de departamento dos dispositivos ou ao reatribuir os valores a departamentos diferentes.

Para alterar os valores de dados do departamento, consulte "Atribuindo Valores de Dados a Um Dispositivo Individual" na página 60. Para alterar o departamento de um grupo de dispositivos, consulte "Atribuindo Valores de Dados a Todos os Dispositivos em um Grupo de Dispositivos" na página 60.

Excluindo um Departamento

IMPORTANTE Não é possível excluir um departamento se houver dispositivos ou grupos associados ao mesmo. Primeiro é necessário remover todos os dispositivos do departamento. Para mais informações, consulte "Removendo Dispositivos de um Departamento" na página 56.

Para excluir um departamento:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.
2. No painel de navegação, clique **Administração** > **Dados** > **Criar e Editar Departamentos**.
3. Na página Criar e Editar Departamentos, na grelha de resultados, clique no link **Editar** para o departamento que você deseja excluir.
4. Clique em **Excluir**.

   A página Criar e Editar Departamentos se atualiza e mostra uma mensagem que confirma que o departamento foi excluído.

Exportando e Importando Dados

É possível exportar (baixar) dados de dispositivos para uso em aplicativos externos, tal como o Microsoft Excel ou para seus sistemas empresariais. A extração de arquivo pode ser em arquivo CSV (Comma Separated Value) ou XML (eXtensible Markup Language). Adicionalmente, você pode editar atributos específicos de dispositivos ou um grupo de dispositivos ao exportar um arquivo de dados CSV, editando-o e depois carregando-o.

Alternativamente, para editar dados de um único dispositivo individual, consulte "Atribuindo Valores de Dados a Um Dispositivo Individual" na página 60. Para atribuir o mesmo valor de atributo a um grupo de dispositivos, consulte "Atribuindo Valores de Dados a Todos os Dispositivos em um Grupo de Dispositivos" na página 60.

O processo de exportar e importar dados no formato CSV segue esta sequência:

- Extraindo Dados para um Arquivo
- Baixando um Arquivo de Extração de Dados
- Editando e Importando um Arquivo de Dados CSV
- Verificando a Importação de Arquivos

Extraindo Dados para um Arquivo

Para extrair dados existentes para um arquivo:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Dados** > **Exportar Dados**.
3. Faça uma das seguintes opções:
   - Para extrair dados de dispositivos para um grupo de dispositivos específico, na página Exportar Dados, abra a lista **O Grupo é** e selecione o grupo de dispositivos para qual você deseja editar dados.
   - Para extrair dados de dispositivos para todos os dispositivos, selecione **Todos os Dispositivos**.
4. Na área de **Nome e Formato**, faço o seguinte:

a) No campo **Nome**, digite um nome para o arquivo de extração de dados.

b) Na lista de **Formato** selecione o formato que você deseja usar.

NOTA Se você pretende editar o arquivo para importação, o formato deve ser **CSV**.

5. Na área de **Criar Alerta de E-mail**, se você deseja receber uma notificação por e-mail quando o arquivo estiver disponível, insira seu endereço de e-mail no campo **Seu Endereço de E-mail**.

6. Clique em**Continuar**.

   A solicitação do arquivo de dados é processada em segundo plano. Quando a solicitação é enviada, a página Exportar Dados se atualiza e exibe um link para o **Status de Exportação de Dados** .

   Quando o status exibir **Pronto**, o relatório está disponível para download. Consulte "Baixando um Arquivo de Extração de Dados" na página 58. Se você tiver fornecido um endereço de email, uma notificação por e-mail é enviada.

Baixando um Arquivo de Extração de Dados

A página Status da Exportação de Dados é usada para baixar um arquivo de extração de dados.

Para baixar um arquivo de extração de dados:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Dados** > **Status de Exportação de Dados**.
3. Na página Status da Exportação de Dados, na coluna de **Status**, clique no link apropriado de **Pronto** para o relatório que você deseja baixar.
4. Clique em **Salvar Como** para salvar o arquivo em um local conhecido do seu computador local.

Editando e Importando um Arquivo de Dados CSV

Para editar e importar um arquivo de dados CSV:

1. Abra o arquivo e edite os valores que você deseja alterar.

   IMPORTANTE **Não edite os cabeçalhos das colunas nem os valores dos identificadores.**

2. **Salve** o arquivo atualizado como um arquivo CSV e fecha-o.
3. Conecte-se à Central do Cliente.
4. No painel de navegação, clique **Administração** > **Dados** > **Importar Dados**.
5. Na página Importar Dados, no campo **Nome**, digite um nome descritivo para identificar este carregamento específico.
6. Caso deseje receber uma notificação de e-mail quando a importação de dados estiver concluída, digite seu endereço de e-mail no campo **E-mail** .
7. No campo **Nome de Arquivo**, insira o caminho completo do arquivo editado ou clique em **Navegar** para selecioná-lo no seu computador local.
8. Clique em **Carregar**.

Uma mensagem aparece, indicando que o arquivo foi carregado com sucesso e a página Importar Dados se abre exibindo um link para o **Status de Importação de Dados**.

O arquivo de dados carregado é processado em segundo plano. Para garantir que suas edições foram corretamente importadas, complete a tarefa, "Verificando a Importação de Arquivos " na página 59.

Se você forneceu um endereço de email, a Central do Cliente envia uma notificação por email quando o upload for concluído.

NOTA É também possível importar dados de dispositivos do Computrace Mobile Theft Management, usando as instruções fornecidas na tarefa, "Importando Dados de Dispositivos iPad para a Central do Cliente." na página 351.

Verificando a Importação de Arquivos

Para verificar que o arquivo foi importado com sucesso:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Administração** > **Dados** > **Status de Importação de Dados**.
3. Na página Status de Importação de Dados, você pode ver o arquivo de dados que foi carregado.

   Se o valor na coluna **Status** exibir **Pronto**, o arquivo de dados está carregado. Clique no link de **Pronto** para ver uma cópia dos dados importados e das mensagens (por linha) que indicam quaisquer erros. Ao concluir a importação, os dados atualizados ficam visíveis em todos os relatórios da Central do Cliente.

Visualizando e Editando Campos de Dados

A Central do Cliente pode guardar informação em campos predefinidos. Poderá também definir até vinte campos de dados únicos adicionais. Os campos predefinidos incluem o seguinte:

- Número do Ativo
- E-mail de Usúario Atribuído
- Nome de Usuário Atribuído
- Data de Aquisição do Computador
- Centro/Código de Custos
- Departamento
- Inativo
- Possui Garantia de Serviço
- Data do fim da concessão
- Número do contrato de concessão
- Responsabilidade do contrato de concessão
- Data de início da concessão
- Fornecedor do contrato de concessão
- Localização Física / Real
- Referência de Ordem de Compra
- Data de término do Contrato de Serviço
- Data de Início do Contrato de Serviço
- Fornecedor do Contrato de Serviço
- Telefone/Extensão do Usuário
- Fornecedor do Contrato de Garantia
- Data de término da Garantia
- Data de Início da Garantia

NOTA Alguns destes campos opcionais podem não ser aplicáveis à sua empresa.

É possível usar a página Visualizar e Editar Campos Definido pelo Usuário para manualmente atribuir valores de campos a dispositivos individuais ou a grupos de dispositivos. Além disso, os usuários da Central do Cliente podem migrar dados armazenados de um dispositivo para outro.

Para atribuir valores de campos a múltiplos dispositivos, consulte "Atribuindo Valores de Dados a Todos os Dispositivos em um Grupo de Dispositivos" na página 60.

Quando dados são preenchidos em Campos definidos pelo Usuário, você pode ver a informação no relatório de ativos ao marcar a caixa de seleção **Com campos definidos pelo usuário**.

Esta seção descreve as seguintes tarefas:

- Atribuindo Valores de Dados a Um Dispositivo Individual
- Atribuindo Valores de Dados a Todos os Dispositivos em um Grupo de Dispositivos
- Trabalhando com Múltiplos Valores

Atribuindo Valores de Dados a Um Dispositivo Individual

Para atribuir valores de dados a um dispositivo individual:

1. Conecta-se à Central do Cliente como um Administrador ou Usuário Avançado
2. No painel de navegação, clique **Administração** > **Dados** > **Ver e Editar Dados de Campos Definidos pelo Usuário**.
3. Na página Ver e Editar Dados de Campos Definidos pelo Usuário, clique em **Escolher Dispositivo**. Um diálogo é aberto e mostra uma lista de todos os Identificadores associados com sua conta.
4. Clique no dispositivo desejado na lista.

   A página Ver e Editar Campos Definidos pelo Usuário é aberta com o Identificador selecionado aparecendo na área **Dados para o Dispositivo**.

   Tanto as tabelas de **Campos Fixos** como as de **Campos definidos pelo Usuário** são atualizadas, mostrando quaisquer valores anteriormente atribuídos a este dispositivo.
5. Na coluna de **Dados do Campo**, digite as informações em cada campo que você deseja definir.
6. Clique em **Salvar Alterações** e no diálogo de confirmação clique em **OK**.

Atribuindo Valores de Dados a Todos os Dispositivos em um Grupo de Dispositivos

Para atribuir valores de dados a todos os dispositivos em um grupo de dispositivos:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.
2. No painel de navegação, clique **Administração** > **Dados** > **Ver e Editar Dados de Campos Definidos pelo Usuário**.
3. Na página Ver e Editar Dados de Campos Definidos pelo Usuário, clique em **Escolher grupo de dispositivos** e selecione o grupo de dispositivos desejado a partir da lista.

   A página Ver e Editar Dados Definidos por Usuários é aberta com o nome do grupo de dispositivos selecionado aparecendo na área **Dados para o Grupo**.

Tanto as tabelas de **Campos Fixos** como as de **Campos definidos pelo Usuário** são atualizadas, mostrando os valores atualmente atribuídos aos dispositivos neste grupo. Se os dispositivos tiverem valores de **Dados de Campos** diferentes, o botão **Múltiplos Valores** aparece. Valores diferentes em um campo de dados não é incomum para dispositivos em vários grupos. Para informações sobre **Múltiplos valores** em um campo de dados, consulte "Trabalhando com Múltiplos Valores" na página 61.

4. Digite as informações no campos que você deseja definir.
5. Clique em **Salvar Alterações** e no diálogo de confirmação clique em **OK**.

Trabalhando com Múltiplos Valores

Um grupo de dispositivos contém, por norma, vários dispositivos e, como um dispositivo tem valores de dados atribuídos a si, cada dispositivo pode ter valores de dados diferentes para o mesmo campo de dados. Você pode querer ignorar valores de dados de campos para alguns ou todos os dispositivos em um grupo de dispositivos particular.

Quando existem valores diferentes para um campo de dados, o valor de **Dados de Campo** mostra um botão etiquetado **Múltiplos Valores.**

Para alterar múltiplos valores em um campo de dados:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.
2. No painel de navegação, clique **Administração** > **Dados** > **Ver e Editar Dados de Campos Definidos pelo Usuário**.
3. Na página Ver e Editar Dados de Campos Definidos pelo Usuário, clique em **Escolher grupo de dispositivos** para abrir o diálogo de seleção de Grupos. Este diálogo fornece a lista de grupos de dispositivos para sua conta.
4. Abrir a lista e selecione o grupo de dispositivos desejado.

   A página Ver e Editar Dados Definidos por Usuários é aberta com o nome do grupo de dispositivos selecionado aparecendo na área **Dados para o Grupo**.

   Tanto as tabelas de **Campos Fixos** como as de **Campos definidos pelo Usuário** são atualizadas, mostrando os valores atualmente atribuídos aos dispositivos neste grupo.
5. Na página Ver e Editar Dados de Campos Definidos pelo Usuário, procure **Múltiplos Valores** na coluna **Dados de Campo** tanto nas áreas de **Campos Fixos** e de **Campos definidos pelo Usuário**.
   - Para cada campo a que você deseja atribuir o mesmo valor, clique em **Múltiplos Valores**.
   - No diálogo Editar Múltiplos Valores, na coluna **Ação**, abra a lista e clique em **Alterar** para cada valor de dados que você deseja atualizar.
   - No diálogo atualizado, no campo **Alterar**, digite as informações apropriadas para cada valor de dados.
   - Clique no botão **Salvar e Fechar** para fazer as alterações e fechar o diálogo.
6. Na página Ver e Editar Dados de Campos Definidos pelo Usuário, clique em **Salvar alterações**.

Migrando Dados Entre Dispositivos

A Central do Cliente suporta três métodos de migrar dados entre dois dispositivos gerenciados:

- Copiando Dados
- Movendo Dados
- Trocando Dados

A seguinte tabela descreve as alterações de dados que ocorrem no Dispositivo A e no Dispositivo B quando você usa os diferentes métodos de migração de dados.

Quando você...	Alterações de dados em:	
	Dispositivo A	**Dispositivo B**
Copiar dados de Dispositivo A para Dispositivo B	Não	Sim
Mover dados de Dispositivo A para Dispositivo B	Sim	Sim
Trocar dados entre Dispositivo A para Dispositivo B	Sim	Sim

Copiando Dados

É possível copiar os valores de um dispositivo (Identificador) para outro, resultando em valores idênticos para ambos os dispositivos.

Exemplo

Dispositivo A possui os dois seguintes campos:

- **Depósito**: 3752
- **ID do edifício**: North28

e o **Dispositivo B** tem os dois campos a seguir:

- **Depósito**: 4788
- **ID do edifício**: Oeste35

Quando os dados desses dois campos forem copiados de **Dispositivo A**para **Dispositivo B**, então os valores originais do **Dispositivo B** serão sobrescritos para corresponder aos do **Dispositivo A**. No final, ambos dispositivos terão dados idênticos nesses dois campos.

- **Depósito**: 3752
- **ID do edifício**: North28

Para copiar dados armazenados de um dispositivo para outro:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Ver e Editar Dados de Campos Definidos pelo Usuário**.
3. Na página Ver e Editar Dados de Campos Definidos pelo Usuário, clique em **Escolher Dispositivo**. Um diálogo é aberto e mostra uma lista de todos os Identificadores associados com sua conta.

   Na lista, clique no dispositivo a partir do qual você deseja copiar os dados. Este dispositivo se torna em sua fonte de dados (**Dispositivo A**).

   A página Ver e Editar Campos Definidos pelo Usuário é atualizada e mostra a informação específica de **Dados para o Dispositivo: <Identificador do Dispositivo A>** nos Campos Fixos e também nos locais dos Campos Definidos pelo Usuário.

4. Clique em **Copiar dados para novo dispositivo**, que abrirá a página Copiar Dados para Outro Dispositivo.
5. Na área **Dispositivo B**, clique em **Selecionar dispositivo para a cópia** para escolher o dispositivo a que você está copiando os dados (**Dispositivo B**).
6. Na lista, clique no dispositivo para selecioná-lo. A página Copiar Dados para Outro Dispositivo se atualiza e exibe as informações específicas deste dispositivo secundário designado como **Dispositivo B**.
7. Faça uma revisão dos detalhes mostrados para o **Dispositivo A** e para o **Dispositivo B** para verificar que você selecionou os dispositivos certos.
8. Selecione os campos de dados para copiar de seguinte forma:
   a) Clique em **Copiar Dados** para abrir a página Copiar.
   b) Marque as caixas de seleção para aqueles campos que você deseja copiar de **Dispositivo A** para **Dispositivo B**.
9. Clique em **Copiar de A para B** para iniciar o processo de cópia.
   a) No diálogo de Aviso, clique em **OK** para continuar.
   b) No diálogo de Confirmação, clique em **OK**.
   c) Na página Copiar, verifique que as informações que pretendia copiar está aparecendo para o **Dispositivo B** e clique **OK**.

   A página Ver e Editar Campos definidos pelo Usuário se atualiza e mostra informações específicas de **Dados para o Dispositivo:<O Identificador do Dispositivo B>** tanto nos locais de Campos Fixos como nos de Campos definidos pelo Usuário.
10. Clique em **Salvar Alterações** e no diálogo de confirmação, clique em **OK**.

    Uma mensagem de confirmação indica que o **Dispositivo B** agora tem os campos copiados de **Dispositivo A**.

Movendo Dados

Mover dados é diferente de copiar dados porque, uma vez concluída a movimentação, os campos de dados associados ao primeiro dispositivo (**Dispositivo A**) são apagados e ficarão em branco.

Exemplo

Dispositivo A possui os dois seguintes campos:

- **Depósito**: 3752
- **ID do edifício**: North28

e o **Dispositivo B** tem os dois campos a seguir:

- **Depósito**: 4788
- **ID do edifício**: Oeste35

Quando os dados desses dois campos forem transferidos de **Dispositivo A** para **Dispositivo B**, os valores originais de **Dispositivo B** serão sobrescritos com os valores de **Dispositivo A** e os valores de **Dispositivo A** são apagados porque foram transferidos.

Quando concluído, os dispositivos terão os seguintes valores:

- **Dispositivo A:**
  - **Depósito:** <nulo>
  - **ID do Edifício:** <nulo>
- **Dispositivo B:**
  - **Depósito**: 3752
  - **ID do edifício**: North28

Para mover dados armazenados de um dispositivo para outro:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Ver e Editar Dados de Campos Definidos pelo Usuário**.
3. Na página Ver e Editar Dados de Campos Definidos pelo Usuário, clique em **Escolher Dispositivo**. Um diálogo é aberto e exibe uma lista de todos os dispositivos associados com sua conta.

   Na lista, clique no dispositivo a partir do qual você deseja mover os dados. Este dispositivo se torna em sua fonte de dados (**Dispositivo A**).

   A página Ver e Editar Campos Definidos pelo Usuário é atualizada e mostra a informação específica de **Dados para o Dispositivo: <Identificador do Dispositivo A>** nos Campos Fixos e também nos locais dos Campos Definidos pelo Usuário.
4. Clique em **Mover dados para novo dispositivo**, que abre a página Mover Dados para Outro Dispositivo.
5. Na área **Dispositivo B**, clique em **Selecionar dispositivo para a transferência** para escolher o dispositivo a que você está movendo os dados (**Dispositivo B**).
6. No diálogo, clique no **Identificador** do dispositivo para selecioná-lo. A página Mover Dados para Outro Dispositivo se atualiza e exibe as informações específicas deste dispositivo secundário designado como **Dispositivo B**.
7. Faça uma revisão dos detalhes mostrados para o **Dispositivo A** e para o **Dispositivo B**para verificar que você selecionou os dispositivos certos.
8. Selecione os campos de dados que você pretende transferir, da seguinte forma:
   a) Clique em **Mover Dados** para abrir a página Mover.
   b) Marque as caixas de seleção para aqueles campos que você deseja mover de **Dispositivo A** para **Dispositivo B**.

9. Clique em **Mover de A para B** para iniciar o processo de transferência de seguinte forma:
   a) No diálogo de Aviso, clique em **OK**.
   b) No diálogo de Confirmação, clique em **OK**.
   c) Na página Mover, verifique que as informações que pretendia mover está aparecendo para o **Dispositivo B** e clique **OK**.

   A página Ver e Editar Campos definidos pelo Usuário se atualiza e mostra informações específicas de **Dados para o Dispositivo:<O Identificador do Dispositivo B>** tanto nos locais de Campos Fixos como nos de Campos definidos pelo Usuário.
10. Clique em **Salvar Alterações** e no diálogo de confirmação, clique em **OK**.

Trocando Dados

Ao migrar dados usando a opção de Trocar Dados, os dois dispositivos selecionados trocam seus valores de dados um com o outro e nenhum retém seus valores originais.

Exemplo

Dispositivo A possui os dois seguintes campos:

- **Depósito**: 3752
- **ID do edifício**: North28

e o **Dispositivo B** tem os dois campos a seguir:

- **Depósito**: 4788
- **ID do edifício**: Oeste35

Quando os dados desses dois campos forem trocados entre **Dispositivo A** e **Dispositivo B**, esses dispositivos ficam com os seguintes valores:

- **Dispositivo A:**
  - **Depósito**: 4788
  - **ID do edifício**: Oeste35
- **Dispositivo B:**
  - **Depósito**: 3752
  - **ID do edifício**: North28

Para trocar dados armazenados de um dispositivo gerenciado para outro:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Ver e Editar Dados de Campos Definidos pelo Usuário**.
3. Na página Ver e Editar Dados de Campos Definidos pelo Usuário, clique em **Escolher Dispositivo**. Um diálogo é aberto e mostra uma lista de todos os Identificadores associados com sua conta.

   Na lista, clique no dispositivo a partir do qual você deseja trocar os dados. Este dispositivo se torna em sua fonte de dados (**Dispositivo A**).

   A página Ver e Editar Campos Definidos pelo Usuário é atualizada e mostra a informação específica de **Dados para o Dispositivo: <Identificador do Dispositivo A>** nos Campos Fixos e também nos locais dos Campos Definidos pelo Usuário.

4. Clique em **Trocar dados com outro dispositivo**, que abre a página Trocar Dados com Outro Dispositivo.
5. Na área **Dispositivo B**, clique em **Selecionar dispositivo para a troca** para escolher o dispositivo com qual você está fazendo a troca de dados (**Dispositivo B**).

   No diálogo, clique no dispositivo para selecioná-lo. A página Trocar Dados com Outro Dispositivo se atualiza e exibe as informações específicas deste dispositivo secundário designado como **Dispositivo B**.
6. Faça uma revisão dos detalhes fornecidos para o **Dispositivo A** e para o **Dispositivo B** para verificar que você selecionou os dispositivos certos.
7. Selecione os campos de dados que você pretende trocar, da seguinte forma:
   a) Clique em **Trocar Dados** para abrir a página Trocar.
   b) Marque as caixas de seleção somente para aqueles campos que você deseja trocar entre os dispositivos.
8. Clique em **Trocar entre A e B** para iniciar o processo de troca.
   a) No diálogo de Confirmação, clique em **OK**.
   b) Na página Trocar, clique em **OK**.

   A página Ver e Editar Campos definidos pelo Usuário se atualiza e mostra informações específicas de **Dados para o Dispositivo:<O Identificador do Dispositivo B>** tanto nos locais de Campos Fixos como nos de Campos definidos pelo Usuário.
9. Clique em **Salvar Alterações** e no diálogo de confirmação, clique em **OK**.

Gerenciando Definições de Campos Fixos e Definidos pelo Usuário

Gerenciando campos definidos pelo usuário envolve a criação, edição e exclusão dos mesmos.

Esta seção descreve as seguintes tarefas:

- Criando Campos Definidos pelo Usuário para Armanezar mais Dados
- Editando uma Definição de Campo Fixo ou Definido pelo Usuário
- Excluindo um Campo Definido pelo Usuário

Criando Campos Definidos pelo Usuário para Armanezar mais Dados

Além dos campos de dados predefinidos, os administradores da Central do Cliente podem definir até 20 campos de dados únicos adicionais.

Para criar um novo campo de dados definido pelo usuário:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Gerenciar Campos Definidos pelo Usuário**.
3. Na página Gerenciar Campos Definidos pelo Usuário, clique em **Criar campo definido pelo usuário**.
4. Na página Criar Campo Definido pelo Usuário, no campo **Etiqueta do Campo**, digite um nome para seu novo ponto (de dados) de identificação.
5. Selecione a opção de **Tipo de Campo** apropriado a partir dos seguintes valores:

- **Texto (50)** aceita texto simples com até 50 caracteres de comprimento.
- **Data** aceita valores de data na forma d/m/aaaa
- **Lista Suspensa** aceita valores especificados de uma lista fornecida.

Quando este tipo de campo é selecionado, a página Criar Campo Definido pelo Usuário se atualiza e inclui o campo **Valores de Lista Suspensa**. Use este campo para inserir os valores que aparecem na lista suspensa do campo. Separe os vários valores diferentes que deseja incluir na lista com uma vírgula.

6. Se você deseja permitir a edição de campos por Usuários Avançados, na área **Edição de Campos** marque a caixa de seleção **Editável por Usuário Avançado**.
7. Clique em **Salvar**, que atualiza a página Gerenciar Campos Definidos pelo Usuário. Na área **Campos Definidos pelo Usuário**, faça uma revisão à lista para ver o novo campo definido pelo usuário que você criou.

Editando uma Definição de Campo Fixo ou Definido pelo Usuário

Para editar uma definição de campo fixo ou definido pelo usuário:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Gerenciar Campos Definidos pelo Usuário**.
3. Na página Gerenciar Campos Definidos pelo Usuário, clique no link **Editar** que está associado ao campo de dados que você deseja alterar.

NOTA Não é possível editar campos fixos que têm um asterisco (*) a seguir ao Rótulo de Campo.

4. Faça uma das seguintes opções:
   - Para editar um campo fixo, na página Editar Campo Definido pelo Usuário, na área **Campo Fixo**, faça o seguinte:

     IMPORTANTE O campo **Etiqueta do Campo** e as opções de **Tipo de Campo** não estão disponíveis para edição. Se você deseja alterar estas informações, você precisa **Excluir** o campo definido pelo usuário e criar um novo com as informações apropriadas.

     i) Na opção **Edição de Campos**, indique se usuários avançados podem editar ou não este campo fixo.

     ii) Clique em **Salvar alterações** para salvar as alterações e retornar para a página Gerenciar Campos definidos pelo Usuário, onde você pode verificar que a alteração foi feita.
   - Para editar um campo definido pelo usuário, na página Editar Campo Definido pelo Usuário, na área **Campo Definido pelo Usuário**, faça o seguinte:

     i) No campo **Etiqueta do Campo**, altere o nome conforme apropriado.

     IMPORTANTE As opções **Tipo de Campo** não estão disponíveis para edição. Se você deseja alterar estas informações, você precisa **Excluir** o campo definido pelo usuário e criar um novo com as informações apropriadas.

ii) Na opção **Edição de Campos**, indique se usuários avançados podem editar ou não este campo definido pelo usuário.

NOTA É possível apenas editar a opção de Edição de Campos para Campos Fixos.

iii) Clique em **Salvar alterações** para salvar as alterações e retornar para a página Gerenciar Campos definidos pelo Usuário, onde você pode verificar que a alteração foi feita.

Excluindo um Campo Definido pelo Usuário

Para excluir um campo definido pelo usuário:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Gerenciar Campos Definidos pelo Usuário**.
3. Na página Gerenciar Campos Definidos pelo Usuário, na área **Campos Definidos pelo Usuário**, clique no link **Editar** que está associado ao campo que você deseja excluir.
4. Na página Editar Campo Definido pelo Usuário, clique em **Excluir**.
5. No diálogo de Confirmação, clique em **OK** para excluir este campo. A página Gerenciar Campos Definidos pelo Usuário se atualiza e este campo definido pelo usuário é excluído.

Usando Mensagens do Usuário Final

O recurso de Mensagens do Usuário Final permite aos administradores da Central do Cliente comunicar com usuários finais de dispositivos gerenciados através de mensagens URL ou personalizadas. As Mensagens do Usuário Final ocorrem durante a chamada de agente para o Centro de Monitoramento. Administradores podem também solicitar informações de usuários finais através de mensagens do usuário final que preenche campos definidos pelo usuário. Para mais informações, consulte "Gerenciando Definições de Campos Fixos e Definidos pelo Usuário" na página 66.

Os administradores podem criar qualquer número de mensagens do usuário final e implantá-las em todos os dispositivos de sua empresa, num grupo de dispositivos específico ou em um dispositivo particular.

Existem dois tipos de mensagens de usuário final:

- Mensagens personalizadas que podem solicitar dados de usuários finais. Consulte "Criando Mensagens do Usuário Final Personalizadas" na página 69.
- Mensagens de URL que abrem as janelas do navegador dos usuários finais em um site específico. Consulte "Criando Mensagens URL do Usuário Final" na página 71.

As Mensagens do Usuário Final estão apenas disponíveis em dispositivos rodando os seguintes sistemas operacionais suportados:

- Sistemas operacionais do Windows com o Internet Explorer
- Sistemas operacionais Mac

Esta seção descreve as seguintes tarefas:

- Criando Mensagens do Usuário Final
- Visualizando Mensagens do Usuário Final
- Editando Mensagens do Usuário Final

- Ativando uma Mensagem de Usuário Final
- Suspendendo uma Mensagem de Usuário Final
- Visualizando Reconhecimentos de Mensagens do Usuário Final
- Reenviando Mensagens do Usuário Final
- Excluindo Mensagens do Usuário Final

Criando Mensagens do Usuário Final

Esta seção descreve as seguintes tarefas:

- Criando Mensagens do Usuário Final Personalizadas
- Criando Mensagens URL do Usuário Final

Criando Mensagens do Usuário Final Personalizadas

Para criar uma mensagem de usuário final personalizada:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Mensagens do Usuário Final**. A página Mensagens do Usuário Final mostra uma lista de mensagens do usuário final.
3. Clique em **Criar Novas Mensagens de Usuário Final**.
4. Na página Criar Mensagem de Usuário Final, na área de **Informação da mensagem**, no campo **Nome de Mensagem**, digite um nome descritivo para a nova mensagem. Este nome de mensagem é apenas para sua referência e não será mostrado ao usuário final.
5. Na área **Conteúdo da mensagem**, complete as seguintes informações:
   a) Nas opções **Tipo de Mensagem**, clique na opção **Mensagem Personalizada**.
   b) No campo **Título de Mensagem** digite o título que deseja que seja exibido na barra do título da mensagem enviada para usuários finais.
   c) No campo **Texto da Mensagem** você pode inserir textos e links de URL, bem como os seguintes tags HTML:

<a>	<b>	<i>	<u>
<font>	<p>	 	

   d) Se você deseja incluir uma imagem com sua mensagem, faça o seguinte:
      - Insira o **URL de Imagem** para a imagem que você deseja que seja exibida.
      - Abra a lista **Local de Exibição da Imagem** e selecione onde você deseja que a imagem apareça na mensagem.
      - No campo **Hiperlink de Imagem**, insira ou cole o hiperlink apropriado para a imagem que você pretende mostrar.

      Você está limitado a uma imagem por mensagem.
   e) Se você estiver solicitando informações de seus usuários finais, clique em **Escolher campos**, que abre o diálogo de Campos Personalizados. A coluna esquerda da caixa de diálogo exibe todos os **Campos Disponíveis** que podem ser adicionados à mensagem. A coluna direita do diálogo fornece uma lista de todos os **Campos Selecionados** atualmente.

Na lista dos **Campos Disponíveis**, clique nos campos que deseja incluir na mensagem e clique **>** para movê-los para a lista dos **Campos Selecionados**. Clique em **>>** para mover todos os campos disponíveis para a lista de **Campos Selecionados**. Se, por engano, você mover um campo disponível para a lista de **Campos Selecionadas**, poderá selecioná-lo e clicar em **<** para movê-lo de volta para a lista de **Campos Disponíveis**. Ao concluir, clique em **OK**.

O diálogo Campos fecha e a página Criar Mensagens do Usuário Final se atualiza e mostra os **Campos Selecionados** como uma lista de caixas de seleção na área **Campos Incluídos**.

f) Sob o cabeçalho de **Obrigatório**, marque a caixa de seleção para cada campo que você deseja especificar como obrigatório.

O usuário final precisa fornecer informações para estes campos obrigatórios para poder enviar com sucesso uma resposta à mensagem do usuário final.

6. Na área de **Destino de mensagem** na área **Enviar Para**, indica a opção apropriada que define os dispositivos que recebem a mensagem da seguinte forma:

   - Clique em **Todos os Dispositivos** para enviar a mensagem do usuário final a todos os dispositivos, que inclui ativações futuras.
   - Clique em **Dispositivo Específico**, clique em **Escolher dispositivo** e depois selecione o dispositivo que você deseja que receba a mensagem do usuário final.
   - Clique em **Grupo Específico**, clique em **Escolher grupo** e depois selecione o **Nome do Grupo** que você pretende que receba a mensagem do usuário final. Qualquer dispositivo adicionado ou removido deste grupo é de forma semelhante adicionado a ou removido da mensagem. Você deve definir o grupo de dispositivos antes de poder selecioná-lo. Para mais informações, consulte "Criando um Novo Grupo de Dispositivos" na página 79.

   IMPORTANTE Quando uma mensagem de usuário final é aplicada a um **grupo específico**, qualquer dispositivo adicionado ou removido desse grupo é igualmente associado ou desassociado à mensagem do usuário final.

7. Na área de **Exibição de Mensagens**, nas opções para **Critérios de Exibição de Mensagens (Regras)**, selecione a opção que define a frequência com que a mensagem é apresentada a usuários finais a partir das seguintes opções disponíveis:

   - **Na próxima chamada** apresenta a mensagem a usuários finais na próxima chamada do dispositivo para o Centro de Monitoramento.
   - **Em ou Depois** abre um campo onde você insere a data ou pode clicar no ícone do **Calendário** para selecionar a data que deseja para enviar a mensagem.

8. Faça uma revisão à mensagem que você criou e depois escolha umas das seguintes opções para salvar a mensagem:

   - Clique em **Salvar e Ativar**. A mensagem é ativada e exibida em dispositivos que se qualificam de acordo com a opção de Exibição de Mensagens.
   - Clique em **Salvar e Suspender** para pré-visualizar a mensagem. Antes de a ativar, consulte "Visualizando Mensagens do Usuário Final" na página 72. Nenhum dispositivo receberá esta mensagem até você ativar a mensagem. Esta opção é recomendada.

A página Mensagens do Usuário Final atualiza a grelha de resultados para incluir a nova mensagem de usuário final personalizada.

Criando Mensagens URL do Usuário Final

Uma mensagem de URL exibe qualquer endereço da World Wide Web no navegador do usuário final. A Central do Cliente não registra quando o usuário final confirma o recebimento de uma mensagem de URL.

Para criar uma mensagem de URL:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Mensagens do Usuário Final**.
3. Na página Mensagens do Usuário Final, clique em **Criar nova mensagem de usuário final**.
4. Na página Criar Mensagem de Usuário Final, na área de **Informação da mensagem**, no campo **Nome de Mensagem**, digite um nome descritivo para a nova mensagem. Este nome de mensagem é apenas para sua referência e não será mostrado ao usuário.
5. Na área **Conteúdo da mensagem**, faça o seguinte:
   a) Clique na opção de **URL** e digite o endereço, incluindo o protocolo; por exemplo, **http://**.
   b) Selecione uma das seguintes opções para a entrega de sua mensagem do usuário final:
      - **Tentar enviar uma vez** indica que a mensagem é enviada apenas uma vez, na próxima chamada do agente.
      - **Enviar repetidamente** indica que a mensagem é enviada em todas as chamadas de agente.

        Esta frequência é útil quando o usuário final tiver se desconectado de um dispositivo e falhado em devolvê-lo até sua data de vencimento. Quando o dispositivo for devolvido, você pode suspender ou excluir a mensagem.
6. Na área de **Destino de mensagem** na área **Enviar Para**, indica a opção apropriada que define os dispositivos que recebem a mensagem da seguinte forma:
   - Para enviar a mensagem do usuário final para todos os dispositivos, incluindo ativações futuras, clique em **Todos os Dispositivos**
   - Para enviar a mensagem do usuário final a um único dispositivo, clique em **Dispositivo Específico**, clique em **Escolher dispositivo** e depois selecione o dispositivo.
   - Para enviar a mensagem do usuário final a todos os dispositivos em um grupo de dispositivos, clique em **Grupo Específico**, clique em **Escolher grupo** e depois selecione o **Nome do Grupo** que você pretende que receba a mensagem de usuário final. Você deve definir o grupo antes de poder selecioná-lo. Para mais informações, consulte "Criando um Novo Grupo de Dispositivos" na página 79.

   IMPORTANTE Quando uma mensagem de usuário final é aplicada a um **grupo específico**, qualquer dispositivo adicionado ou removido desse grupo é igualmente associado ou desassociado à mensagem do usuário final.
7. Na área de **Exibição de Mensagens**, nas opções para **Critérios de Exibição de Mensagens (Regras)**, selecione a opção que define a frequência com que a pagina da Web é apresentada a usuários finais a partir das seguintes opções disponíveis:
   - **Na próxima chamada** apresenta a página da Web a usuários finais na próxima chamada do dispositivo para o Centro de Monitoramento.

- **Em ou Depois** abre um campo onde você insere a data ou pode clicar no ícone do **Calendário** para selecionar a data que deseja para enviar a mensagem.

8. Faça uma revisão à mensagem que você criou e salve-a usando uma das seguintes opções:
   - Clique em **Salvar e Ativar** para salvar a mensagem e ativá-la imediatamente.
   - Clique em **Salvar e Suspender** para salvar e suspender a mensagem. É possível ativar a mensagem posteriormente.

   A página Mensagens do Usuário Final se atualiza e mostra a nova mensagem URL na grelha de resultados, que exibe uma lista de mensagens do usuário final.

Visualizando Mensagens do Usuário Final

Depois de você criar uma mensagem de usuário final personalizada ou de URL, previsualize a mensagem antes de a enviar a usuários finais.

Para previsualizar uma mensagem do usuário final:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Mensagens do Usuário Final**.
3. Na página Mensagens do Usuário Final, na grelha de resultados, clique no link **Nome da Mensagem** para a mensagem que você deseja previsualizar.
4. Na página Criar Mensagem de Usuário Final , clique **Pré-visualizar em Nova Janela** para abrir a mensagem em um nova janela.

   NOTA Certifique-se de que seu navegador esteja configurado para permitir popups.

   Reveja a mensagem e feche a janela.
5. Escolha a partir de uma das seguintes opções:
   - Editar a mensagem. Consulte "Editando Mensagens do Usuário Final" na página 72.
   - Clique em **Salvar e Ativar**. A mensagem é exibida em dispositivos que se qualificam na sua próxima chamada de agente.
   - Clique em **Salvar e Suspender**. Nenhum dispositivo receberá esta mensagem até você ativar a mensagem.

Editando Mensagens do Usuário Final

Esta seção descreve as seguintes tarefas:

- Editando uma Mensagem do Usuário Final Personalizada
- Editando uma Mensagem URL do Usuário Final

Editando uma Mensagem do Usuário Final Personalizada

Para editar uma mensagem de usuário final personalizada existente:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Mensagens do Usuário Final**.

3. Na página Mensagens do Usuário Final, na grelha de resultados, clique em**Nome de Mensagem** ou no link **Editar** da mensagem **Ativa** que você deseja editar. (Não é possível editar uma mensagem **Suspensa**.)
4. Na página Criar Mensagem de Usuário Final, faça as alterações desejadas à mensagem da seguinte forma:
   a) Na área **Informação de Mensagem** no campo **Nome de Mensagem**, digite as informações apropriadas.
   b) Na área do **Status da Mensagem**, clique em **Suspender** para poder fazer estas alterações antes dos dispositivos aplicáveis fazerem uma chamada para o Centro de Monitoramento.
   c) Na área de**Conteúdo da mensagem**, na área de **Tipo de Mensagem**, na opção **Mensagem personalizada**, faça o seguinte:
      - Clique no campo **Título da Mensagem** e digite as informações atualizadas.
      - Clique no campo **Texto da Mensagem** e digite as atualizações apropriadas.
      - Se você desejar usar uma imagem diferente, insira as informações apropriadas no campo **URL de imagem**, abra a lista para **Local de Exibição da Imagem** e selecione a opção correta e no campo **Hiperlink da Imagem** digite as informações atualizadas.
   d) Se você estiver editando as informações que solicitou de seus usuários finais, clique **Escolher campos**, que abre o diálogo de Campos Personalizados.

      A coluna esquerda da caixa de diálogo exibe todos os **Campos Disponíveis** que podem ser adicionados à mensagem. A coluna direita do diálogo fornece uma lista de todos os **Campos Selecionados** atualmente.

      Clique nos campos que você pretende incluir na mensagem e clique **>** para os mover para a lista de **Campos Selecionados**. Clique em **>>** para mover todos os campos disponíveis para a lista de **Campos Selecionados**. Se, por engano, você mover um campo disponível para a lista de **Campos Selecionadas**, poderá selecioná-lo e clicar em **<** para movê-lo de volta para a lista de **Campos Disponíveis**. Quando terminar, clique em **OK**.

      O diálogo Campos fecha e a página Mensagens do Usuário Final se atualiza e mostra os **Campos Selecionados** como uma lista de caixas de seleção no local das opções **Campos Incluídos**.
   e) Marque a caixa de seleção **Obrigatório** para cada campo que você deseja especificar como mandatário.

      O usuário final precisa fornecer informações para esses campos para poder enviar com sucesso uma resposta à mensagem do usuário final.
   f) Clique em **OK**.

      O diálogo Campos fecha e a página Mensagens do Usuário Final se atualiza e mostra os **Campos Selecionados** como uma lista de caixas de seleção no local das opções **Campos Incluídos**.
   g) Marque a caixa de seleção **Obrigatório** para cada campo que você deseja especificar como mandatário.

      O usuário final precisa fornecer informações para esses campos para poder enviar com sucesso uma resposta à mensagem do usuário final.
5. Na área **Destino da mensagem**, nas opções de **Enviar Para**, defina os usuários finais que recebem a mensagem da seguinte forma:

- Para enviar a mensagem do usuário final para todos os dispositivos, incluindo ativações futuras, clique em **Todos os Dispositivos**
- Para enviar a mensagem do usuário final a um único dispositivo, clique em **Dispositivo Específico**, clique em **Escolher dispositivo** e depois selecione o dispositivo.
- Para enviar a mensagem do usuário final a todos os dispositivos em um grupo de dispositivos, clique em **Grupo Específico**, clique em **Escolher grupo** e depois selecione o **Nome do Grupo** que você pretende que receba a mensagem de usuário final. Você deve definir o grupo antes de poder selecioná-lo. Para mais informações, consulte "Criando um Novo Grupo de Dispositivos" na página 79.

IMPORTANTE Quando uma mensagem de usuário final é aplicada a um **grupo específico**, qualquer dispositivo adicionado ou removido desse grupo é igualmente associado ou desassociado à mensagem do usuário final.

6. No local de exibição de mensagens, nas opções **Critérios de Exibição de Mensagens (Regras)**, selecione a opção que define a frequência com que a pagina da Web é apresentada a usuários finais a partir das seguintes opções disponíveis:
   - **Na próxima chamada** apresenta a página da Web a usuários finais apenas uma vez, que é na próxima chamada do dispositivo para o Centro de Monitoramento.
   - **Em ou Depois** abre um diálogo de calendário onde você seleciona a data que deseja para enviar a mensagem.

   Deixe a caixa de seleção de **Reenviar** desmarcada. Para mais informações, consulte "Reenviando Mensagens do Usuário Final" na página 78.
7. Reveja as alterações que você fez a esta mensagem. Você tem as seguintes opções para salvar a mensagem:
   - Clique em **Salvar e Ativar** para salvar a mensagem e ativá-la imediatamente.

     A página Mensagens do Usuário Final atualiza a grelha de resultados com uma lista de mensagens do usuário final que inclui a mensagem que você editou. Tome nota de que o **Status** foi alterado para **Ativo**.
   - Clique em **Salvar e Suspender** para salvar e suspender a mensagem. É possível ativar a mensagem posteriormente.

     A página Mensagens do Usuário Final atualiza a grelha de resultados com uma lista de mensagens do usuário final que inclui a mensagem que você editou. Tome nota de que o **Status** é **Suspenso**.

Editando uma Mensagem URL do Usuário Final

Para editar uma mensagem URL de usuário final:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Mensagens do Usuário Final**.
3. Na página Mensagens do Usuário Final, na grelha, clique em **Nome de Mensagem** ou no link **Editar** da mensagem que você deseja editar.
4. Na página Criar Mensagem de Usuário Final , na área **Informação de Mensagem**, faça as alterações desejadas à mensagem da seguinte forma:
   a) No campo **Nome de Mensagem**, insira as informações apropriadas.

b) No local do Status da Mensagem, clique em **Suspender** para poder fazer estas alterações antes dos dispositivos aplicáveis fazerem uma chamada para o Centro de Monitoramento.

5. Na área de **Conteúdo da mensagem**, nas opções para **Tipo de Mensagem**, no campo da opção de **URL**, faça o seguinte:

a) No campo, digite o endereço, incluindo o protocolo; por exemplo, **http://**.

b) Selecione uma das seguintes opções para a entrega de sua mensagem do usuário final:

- **Tentar enviar uma vez** indica que a mensagem é enviada apenas uma vez, na próxima chamada do agente.
- **Enviar repetidamente** indica que a mensagem é enviada em todas as chamadas de agente.

  Esta frequência é útil quando o usuário final tiver se desconectado de um dispositivo e falhado em devolvê-lo até sua data de vencimento. Quando o dispositivo for devolvido, você pode suspender ou excluir a mensagem.

6. No local do destino da Mensagem, nas opções de **Enviar Para**, defina os usuários finais que recebem a mensagem da seguinte forma:

- Para enviar a mensagem do usuário final para todos os dispositivos, incluindo ativações futuras, clique em **Todos os Dispositivos**
- Para enviar a mensagem do usuário final a um único dispositivo, clique em **Dispositivo Específico**, clique em **Escolher dispositivo** e depois selecione o dispositivo.
- Para enviar a mensagem do usuário final a todos os dispositivos em um grupo de dispositivos, clique em **Grupo Específico**, clique em **Escolher grupo** e depois selecione o **Nome do Grupo** que você pretende que receba a mensagem de usuário final. Você deve definir o grupo antes de poder selecioná-lo. Para mais informações, consulte "Criando um Novo Grupo de Dispositivos" na página 79.

IMPORTANTE Quando uma mensagem de usuário final é aplicada a um **grupo específico**, qualquer dispositivo adicionado ou removido desse grupo é igualmente associado ou desassociado à mensagem do usuário final.

7. No local de exibição de mensagens, nas opções **Critérios de Exibição de Mensagens (Regras)**, selecione a opção que define a frequência com que a pagina da Web é apresentada a usuários finais a partir das seguintes opções disponíveis:

- **Na próxima chamada** apresenta a página da Web a usuários finais na próxima chamada do dispositivo para o Centro de Monitoramento.
- **Em ou Depois** abre um diálogo de calendário onde você seleciona a data que deseja para enviar a mensagem.
- A caixa de seleção de **Reenviar** permite que você reenvie mensagens que já foram enviadas e reconhecidas. Para mais informações, consulte "Reenviando Mensagens do Usuário Final" na página 78.

8. Reveja as alterações que você fez a esta mensagem. Você tem as seguintes opções para salvar a mensagem:

- Clique em **Salvar e Ativar** para salvar a mensagem e ativá-la imediatamente.

  A página Mensagens do Usuário Final atualiza a grelha de resultados com uma lista de mensagens do usuário final que inclui a mensagem que você editou. Tome nota de que o **Status** foi alterado para **Ativo**.

- Clique em **Salvar e Suspender** para salvar e suspender a mensagem. É possível ativar a mensagem posteriormente.

  A página Mensagens do Usuário Final atualiza a grelha de resultados com uma lista de mensagens do usuário final que inclui a mensagem que você editou. Tome nota de que o **Status** é **Suspenso**.

Ativando uma Mensagem de Usuário Final

Apenas mensagens do usuário final ativadas são enviadas a dispositivos gerenciados que atendem aos critérios de mensagens.

Paraativar mensagens URL e personalizadas do usuário final:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Mensagens do Usuário Final**.
3. Na página Mensagens do Usuário Final, na grelha de resultados, clique em **Nome de Mensagem** ou no link **Editar** para uma mensagem **Suspensa** que você deseja ativar.
4. Na página Criar Mensagem de Usuário Final clique em **Salvar e ativar**.
5. A página Mensagens do Usuário Final se atualiza. Veja a grelha de resultados para ver que a mensagem que você selecionou agora diz **Ativo** na coluna de **Status**.

Suspendendo uma Mensagem de Usuário Final

É possível suspender mensagens que não pretende enviar a usuários finais temporariamente.

Para suspender uma mensagem do usuário final:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Mensagens do Usuário Final**.
3. Na página Mensagens do Usuário Final, na grelha de resultados, clique em **Nome de Mensagem** ou no link **Editar** para uma mensagem **Ativa** que você deseja suspender.
4. Na página Criar Mensagem de Usuário Final clique em **Salvar e suspender**.
5. A página Mensagens do Usuário Final se atualiza. Veja a grelha de resultados para ver que a mensagem que você selecionou agora diz **Suspenso** na coluna de **Status**.

Visualizando Reconhecimentos de Mensagens do Usuário Final

A Central do Cliente permite que você veja as mensagens do usuário final personalizadas que foram ou não foram reconhecidas por usuários finais. É também possível baixar os detalhes em um relatório. Se você solicitou informações de usuários finais em uma mensagem, você pode rever as respostas. Para aqueles dispositivos que não deram reconhecimento da mensagem, você pode querer realizar uma pesquisa sobre o porquê esse ser o caso.

Para ver reconhecimentos da mensagem do usuário final:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.
2. No painel de navegação, clique **Administração** > **Dados** > **Mensagens do Usuário Final**.

3. Na página Mensagens do Usuário Final, na grelha de resultados, revise a coluna **Dispositivos Reconhecidos**. Os números com hiperlinks exibidos nesta coluna representam o número de dispositivos que reconheceram as respetivas mensagens do usuário final.

   Para ver que dispositivos deram reconhecimento da mensagem de usuário final que você enviou, clique no link numérico.

4. Na página Dispositivos que reconheceram a Mensagem de Usuário Final, você pode ver os dispositivos que responderam à sua mensagem. Se você solicitou informações do usuário final, pode as encontrar aqui.

   Para mais informações sobre este dispositivo e o usuário do dispositivo, clique no **Identificador**.

   No resumo do dispositivo, você pode ver quem deve contatar para receber mais informações ou possivelmente para enviar outra mensagem.

5. Clique no link **Voltar**para voltar à página de Dispositivos que reconheceram a Mensagem de Usuário Final.

6. Para baixar um relatório dos dispositivos que reconheceram a mensagem do usuário final, na parte superior da grelha de resultados, clique no botão de download.

   Na página Solicitar Relatório, complete as seguintes etapas:

   a) No campo **Nome de Relatório**, digite um nome para este relatório que você deseja baixar.
   b) Abra a lista **Formato de Relatório**e selecione um formato de arquivo.
   c) Na área de **Criar Alerta de E-mail**, se você deseja receber uma notificação por e-mail quando o arquivo estiver disponível, insira seu endereço de e-mail no campo **Seu Endereço de E-mail**.
   d) Clique em**Continuar**.

   Quando a sua solicitação for processada, você pode recuperar o arquivo do relatório na página Meus Relatórios. Para informações sobre a recuperação de relatórios, consulte "Baixando Relatórios" na página 150.

7. Clique no link de **Voltar** para voltar à página Mensagens do Usuário Final.

Para visualizar mensagens do usuário final que não foram reconhecidas pelos dispositivos de destino:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.

2. No painel de navegação, clique **Administração** > **Dados** > **Mensagens do Usuário Final**.

3. Na página Mensagens do Usuário Final, na grelha de resultados, revise a coluna **Dispositivos Não Reconhecidos**. Os números com hiperlink exibidos nesta coluna representam o número de dispositivos que não reconheceram as respetivas mensagens do usuário final.

   Para ver que dispositivos não deram reconhecimento da mensagem de usuário final que você enviou, clique no link numérico.

4. Na página Dispositivos que NÃO reconheceram a Mensagem de Usuário Final, você pode ver os dispositivos que falharam em responder. Para mais informações sobre este dispositivo e o usuário do dispositivo, clique no **Identificador**.

   No resumo do dispositivo, você pode ver quem deve contatar para receber mais informações ou possivelmente para enviar outra mensagem.

5. Clique no link **Voltar**para voltar à página Dispositivos que NÃO reconheceram a Mensagem do Usuário Final.

6. Para baixar um relatório dos dispositivos que não reconheceram a mensagem do usuário final, na parte superior da grelha de resultados clique em .

   Na página Solicitar Relatório, complete as seguintes etapas:

   a) No campo **Nome de Relatório**, digite um nome para este relatório que você deseja baixar.
   b) No campo **Formato de Relatório**, abra a lista e selecione um formato de arquivo.
   c) Na área de **Criar Alerta de E-mail**, se você deseja receber uma notificação por e-mail quando o arquivo estiver disponível, insira seu endereço de e-mail no campo **Seu Endereço de E-mail**.
   d) Clique em**Continuar**.

   Quando a sua solicitação for processada, você pode recuperar o arquivo do relatório na página Meus Relatórios. Para informações sobre a recuperação de relatórios, consulte "Baixando Relatórios" na página 150.

7. Clique no link de **Voltar** para voltar à página Mensagens do Usuário Final.

Reenviando Mensagens do Usuário Final

Existem momentos em que é útil reenviar uma mensagem que já foi recebida e confirmada por usuários finais. Por exemplo, você poderia editar uma mensagem personalizada complexa já existente e reenviá-la, em vez de tomar o tempo para criar uma nova mensagem personalizada.

Para reenviar uma mensagem do usuário final:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Mensagens do Usuário Final**.
3. Na página Mensagens do Usuário Final, na grelha de resultados, clique em **Nome de Mensagem** ou no link **Editar** da mensagem que você deseja reenviar.
4. Na página Criar Mensagem de Usuário Final no local de Exibição da Mensagem, marque a caixa de seleção **Reenviar**.
5. Para salvar esta configuração, faça uma das seguintes ações:
   - Clique em **Salvar e Ativar** para salvar a mensagem. Esta mensagem é exibida a dispositivos que se qualificam de acordo com a opção de Exibição da Mensagem .
   - Clique em **Salvar e Suspender** para salvar e suspender a mensagem. É possível ativar a mensagem posteriormente. Nenhum dispositivo receberá esta mensagem até você ativá-la.

Excluindo Mensagens do Usuário Final

Você pode querer excluir as mensagens do usuário final que já não sejam importantes.

Para excluir mensagens do usuário final:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Dados** > **Mensagens do Usuário Final**.
3. Na página Mensagens do Usuário Final, na grelha de resultados, clique em **Nome de Mensagem** ou no link **Editar** da mensagem que você deseja excluir.
4. Na página Criar Mensagem de Usuário Final , clique em **Excluir**.

A página Mensagem do Usuário Final se atualiza com uma mensagem de confirmação indicando que a mensagem que você selecionou foi excluída.

Cercas Geográficas

O recurso de Cercas Geográficas permite que os administradores da Central do Cliente especifiquem limites geográficos, baseados em dados de rastreamento por geolocalização, para ajudar localizar dispositivos gerenciados. As Cercas Geográficas estão disponíveis para todas as contas autorizadas para o recurso de Rastreamento por Geolocalização. Para mais informações, consulte "Acordo de Autorização de Administração de Segurança e da Geolocalização" na página 259.

Os detalhes e tarefas de cercas geográficas são fornecidos no tópico, "Gerenciando Cercas Geográficas" na página 296.

Grupos de Dispositivos

A Central do Cliente permite que você organize dispositivos gerenciados em agrupamentos lógicos que servem seu modelo de negócio. Por exemplo, você pode agrupar computadores por níveis de gerenciamento, por avaliação de riscos de segurança (aqueles laptops que contêm dados confidenciais), por localizações geográficas (tais como o edifício, o piso ou a sala em que os dispositivos se encontram) e por outros critérios.

A página Grupos de Dispositivos possui uma área de filtro na parte superior da página e uma tabela (grelha de resultados) que inclui todos os grupos de dispositivos associados à sua conta. É possível usar os filtros dos Critérios de Pesquisa para localizar o grupo de dispositivos, ou grupos de dispositivos, que você deseja ver.

É possível definir grupos quando filtra relatórios ou quando escolhe dispositivos para alertas ou mensagens do usuário final.

Esta seção descreve as seguintes tarefas:

- Criando um Novo Grupo de Dispositivos
- Visualizando Todos os Grupos de Dispositivos
- Visualizando um Grupo de Dispositivos Específico
- Editando um Grupo de Dispositivos
- Gerenciando Dispositivos em um Grupo de Dispositivos
- Excluindo Grupos de Dispositivos

Criando um Novo Grupo de Dispositivos

Para criar um novo grupo de dispositivos:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Grupos** > **Grupos de Dispositivos**.
3. Na página Grupos de Dispositivos, clique em **Criar novo grupo de dispositivos**.
4. Na página Criar e Editar Grupos de Dispositivos, na área **Informação do Grupo**, faça o seguinte:

a) No campo **Nome de Grupo**, digite um nome para o novo grupo de dispositivos. Clique no link **Verificar Disponibilidade do Nome** para verificar se o nome que você criou não está em uso.

b) No campo **Descrição de Grupo** , digite uma descrição para o grupo de dispositivos.

c) Para garantir que só administradores podem alterar estas informações, na área **Informação de Grupo**, marque a caixa de seleção de **Bloquear como Somente Leitura**. No entanto, para efeitos desta tarefa, a menos que você seja um administrador ou administrador de segurança, não marque esta caixa de seleção. Se esta caixa de seleção estiver ativada, você não pode executar etapa 5 desta tarefa.

d) Clique em **Salvar informações do grupo** para salvar suas informações de grupo do dispositivo e para atualizar a página Criar e Editar Grupo de Dispositivos. Você vê uma linha de confirmação informando que o grupo de dispositivos foi criado com sucesso.

NOTA Quando criados inicialmente, os grupos de dispositivos não têm dispositivos associados a eles.

---

5. Para adicionar dispositivos a este grupo, na área **Membros do Grupo** faça uma das seguintes ações:

- Para selecionar os dispositivos que você deseja adicionar a este grupo de dispositivos de uma lista, clique em **Adicionar Dispositivos**.

  i) No diálogo Escolher Dispositivo(s) para adicionar ao grupo, faça uma das seguintes ações para selecionar os dispositivos:

  - Marque a caixa de seleção ao lado de cada dispositivo que você deseja adicionar ao grupo.
  - Marque a caixa de seleção de **Selecionar Tudo** para selecionar todos os dispositivos que aparecem neste página da tabela.

  NOTA Você pode deslocar-se pelas várias páginas da grelha de resultados como instruído na tarefa . "Deslocando-se Entre as Páginas do Relatório" na página 140.

  ---

  ii) Clique em **Escolher dispositivo(s)**. O diálogo de Escolher Dispositivo(s) para adicionar ao grupo se fecha.

  Na página Criar e Editar Grupo de Dispositivos, você verá uma linha de confirmação informando que o dispositivo foi adicionado com sucesso a este grupo.

  Além disso, a grelha de resultados se atualiza e exibe os dispositivos que você adicionou, com informações específicas para cada dispositivo nas seguintes colunas:

  - **Identificador**, que é um número de série eletrônico atribuído ao agente instalado em cada dispositivo que você selecionou.
  - **Departamento** a que pertence este dispositivo Um Departamento é um atributo criado pelo usuário para um dispositivo que está incluído no filtro de muitos relatórios da Central do Cliente.
  - **Nome de Dispositivo**, que é o nome dado a um dispositivo.
  - **Nome de usuário**, que é um nome único detectado pelo agente para identificar uma pessoa associada a um dispositivo ou que esteja usando o dispositivo.
  - **Marca**, que é o fabricante de um dispositivo.
  - **Número de Modelo**, que é o tipo de produto de um dispositivo.

- **Número de Série**, que é o número de série do dispositivo.
- **Número de Ativo**, que é um identificador alfanumérico de um dispositivo que é inserido por um usuário na Central do Cliente.

NOTA É possível ordenar os resultados em ordem ascendente ou decrescente para cada coluna, exceto os conteúdos da coluna **Identificador**.

iii) Acima da grelha de resultados, no campo ao lado do botão de **Filtrar Membros**, você pode filtrar a lista exibida na grelha de resultados ao inserir um dos seguintes itens para um dispositivo:

- **Identificador**, que é um número de série eletrônico atribuído ao agente instalado em cada dispositivo que você selecionou.
- **Nome de Dispositivo**, que é o nome dado a um dispositivo.
- **Nome de usuário**, que é um nome único detectado pelo agente para identificar uma pessoa associada a um dispositivo ou que esteja usando o dispositivo.
- **Número de Série**, que é o número de série do dispositivo.

Clique em **Filtrar Membros** e a grelha de resultados se atualiza e exibe uma lista de dispositivos baseado na sua seleção de filtro.

- Para adicionar dispositivos ao grupo ao especificar dispositivos em um arquivo de texto manualmente, clique em **Carregar uma lista de dispositivos**.

IMPORTANTE Números de série Lenovo com sete caracteres podem ser associados com mais de um dispositivo e pode causar erros quando você carrega uma lista de dispositivos usando um arquivo de texto. Quando você carrega uma lista de dispositivos Lenovo, use números de série completos ou os **Identificadores** de dispositivo Computrace, ambos os quais são únicos para cada dispositivo gerenciado.

i) No diálogo Carregar Lista de Dispositivos para Grupo de Dispositivos, sob a área **Carregar Listas de Números de Série ou Identificadores**, no campo **Caminho do Arquivo**, clique em **Navegar** e procure a localização do arquivo que você deseja carregar.

É possível inserir uma lista de dispositivos em uma única coluna, separando cada entrada com uma linha nova (pressione `Enter`). Não utilize pontuação. Clique **Abrir** para selecionar este caminho de arquivo.

ii) Na área de **Tipo de Lista de Arquivos**, clique em uma das seguintes opções:

- **Números de Série**
- **Identificadores**

iii) Clique em **Carregar Arquivo**. Siga as instruções fornecidas na tela para continuar com este procedimento.

Os dispositivos são adicionados ao grupo de dispositivos.

6. Clique no link de **<< Voltar** para fechar esta página e abrir a página Grupos de Dispositivos.

Visualizando Todos os Grupos de Dispositivos

Para visualizar todos os grupos de dispositivos:

1. Conecte-se à Central do Cliente.

2. No painel de navegação, clique em **Administração** > **Grupos** > **Grupos de Dispositivos**.

   Na página Grupos de Dispositivos, veja a grelha de resultados, que mostra todos os grupos de dispositivos que pertencem à sua conta.

   NOTA Se você estiver conectado como um Usuário Avançado ou um Convidado, só pode ver aqueles grupos de dispositivos a que foi atribuído.

Visualizando um Grupo de Dispositivos Específico

Para usar filtros para localizar e visualizar um grupo de dispositivos específico:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Administração** > **Grupos** > **Grupos de Dispositivos**.
3. Na página Grupos de Dispositivos, filtre seus dados para mostrar um grupo de dispositivos específico usando o campo **Critérios de Pesquisa** da seguinte forma:
   - No campo **o Nome do Grupo é ou contém**, digite o nome do grupo de dispositivos que você deseja ver.
   - No campo **a Descrição do Grupo é ou contém**, insira várias letras que você sabe estão na descrição do grupo de dispositivos que você deseja ver.
   - Abra a lista **ou o Grupo contém um Dispositivo onde o campo** e selecione o campo desejado a partir do seguinte:
     - **Qualquer campo**
     - **Identificador**
     - **Nome de Dispositivo**
     - **Nome de usuário**
   - No campo **é ou contém**, use **Escolher** ou insira o valor apropriado para o grupo de dispositivos que você deseja visualizar.
4. Clique em **Mostrar Resultados** para atualizar a grelha de resultados. Se você estiver conectado como um Usuário Avançado ou um Convidado, apenas aqueles grupos de dispositivos a que você foi atribuído são incluídos nos resultados.

   As colunas fornecem as seguintes informações:
   - **Nome do Grupo de Dispositivos** é o nome do grupo.
   - **Contagem** mostra quantos dispositivos estão neste grupo.
   - **Descrição** para este grupo, que você forneceu quando o criou.
   - **Criado por** mostra quem criou este grupo.
   - **Última Modificação** fornece os dados de quando este grupo de dispositivos foi criado ou quando o mesmo foi editado.

Editando um Grupo de Dispositivos

Para editar as informações de um grupo de dispositivos:

1. Conecte-se à Central do Cliente como um administrador e complete a tarefa, "Visualizando um Grupo de Dispositivos Específico" na página 82.

2. Abra a página Criar e Editar Grupos de Dispositivo com os detalhes do grupo de dispositivos que você deseja editar de uma das seguintes formas:
   - Filtre a grelha de resultados para mostrar um grupo de dispositivos particular. Consulte "Visualizando um Grupo de Dispositivos Específico" na página 82.
   - Na grelha de resultados, clique no link **Nome do Grupo de Dispositivos** para o grupo de dispositivos que você deseja editar
3. No local de informações de grupo, você pode editar os seguintes detalhes:
   a) No campo **Nome de Grupo**, insira um nome de grupo para este grupo. Clique no link **Verificar Disponibilidade do Nome** para verificar se o nome que você deseja não está em uso.
   b) No campo **Descrição do Grupo**, edite uma descrição apropriada para o grupo, se desejar alterá-la.
   c) Marque ou desmarque a caixa de seleção **Bloquear como Apenas Leitura**.
   d) Clique em **Salvar** para salvar suas alterações às informações do grupo e atualizar a página Criar e Editar Grupo de Dispositivos.

   Você vê uma linha de confirmação informando que o grupo de dispositivos foi atualizado com sucesso.
4. Se desejar adicionar mais dispositivos a este grupo de dispositivos, consulte "Adicionando Dispositivos a um Grupo de Dispositivos" na página 84.

   É também possível remover dispositivos selecionados do grupo. Para mais informações, consulte "Removendo Dispositivos de um Grupo de Dispositivos" na página 90.

Gerenciando Dispositivos em um Grupo de Dispositivos

É possível usar a página Grupo de Dispositivos para gerenciar a associação a Grupos de Dispositivos, o que inclui as seguintes tarefas:

- Associando dispositivos a Grupos de Dispositivos
- Visualizando os Dispositivos em um Grupo de Dispositivos
- Removendo Dispositivos de um Grupo de Dispositivos

Associando dispositivos a Grupos de Dispositivos

Depois de ter criado grupos de dispositivos, você pode adicionar dispositivos gerenciados a um ou mais grupos de dispositivos.

Há várias maneiras para associar dispositivos com grupos de dispositivos, incluindo:

- Adicionando Dispositivos a um Grupo de Dispositivos
- Adicionando Dispositivos a um Grupo de Dispositivos Automaticamente com base em Endereços IP Locais
- Usando Carregamentos em Massa para Alterar as Associações a Grupos de Dispositivos

Ao adicionar dispositivos a grupos de dispositivos, mantenha os seguintes itens em mente:

- É possível associar dispositivos a mais de um grupo de dispositivos.

- Se você pretende excluir um grupo de dispositivos, precisa remover todos os dispositivos desse grupo primeiro, associar os dispositivos com outro grupo de dispositivos, caso seja apropriado, e só depois excluir o grupo de dispositivos. Para mais informações, consulte os seguintes tópicos:
  - "Removendo Dispositivos de um Grupo de Dispositivos" na página 90
  - "Excluindo Grupos de Dispositivos" na página 91

Adicionando Dispositivos a um Grupo de Dispositivos

Para adicionar dispositivos a um grupo de dispositivos:

1. Conecte-se à Central do Cliente como um Administrador e complete a tarefa, "Visualizando um Grupo de Dispositivos Específico" na página 82.
2. Na grelha de resultados da página Grupos de Dispositivos, clique no **Nome de Grupo de Dispositivos** para qual você desejar adicionar dispositivos.
3. Para adicionar dispositivos a este grupo, na área **Membros do Grupo** faça uma das seguintes ações:
   - Para selecionar os dispositivos que você deseja adicionar a este grupo de dispositivos de uma lista, clique em **Adicionar Dispositivos**.

     i) No diálogo Escolher Dispositivo(s) para adicionar ao grupo, faça uma das seguintes ações para selecionar os dispositivos:
       - Marque a caixa de seleção ao lado de cada dispositivo que você deseja adicionar ao grupo.
       - Marque a caixa de seleção de **Selecionar Tudo** para selecionar todos os dispositivos que aparecem neste página da tabela.

     NOTA Você pode deslocar-se pelas várias páginas da grelha de resultados como instruído na tarefa, "Deslocando-se Entre as Páginas do Relatório" na página 140.

     ii) Clique em **Escolher dispositivo(s)**. O diálogo de Escolher Dispositivo(s) para adicionar ao grupo se fecha.

     Na página Criar e Editar Grupo de Dispositivos, você verá uma linha de confirmação informando que os dispositivos foram adicionados com sucesso a este grupo.

     Além disso, a grelha de resultados se atualiza e exibe os dispositivos que você adicionou, com informações específicas para cada dispositivo nas seguintes colunas:
       - **Identificador**, que é um número de série eletrônico atribuído ao agente instalado em cada dispositivo que você selecionou.
       - **Departamento** a que pertence este dispositivo Um Departamento é um atributo criado pelo usuário para um dispositivo que está incluído no filtro de muitos relatórios da Central do Cliente.
       - **Nome de Dispositivo**, que é o nome dado a um dispositivo.
       - **Nome de usuário**, que é um nome único detectado pelo agente para identificar uma pessoa associada a um dispositivo ou que esteja usando o dispositivo.
       - **Marca**, que é o fabricante de um dispositivo.
       - **Número de Modelo**, que é o tipo de produto de um dispositivo.
       - **Número de Série**, que é o número de série do dispositivo.

- **Número de Ativo**, que é um identificador alfanumérico de um dispositivo que é inserido por um usuário na Central do Cliente.

NOTA É possível ordenar os resultados em ordem ascendente ou decrescente para cada coluna, exceto os conteúdos da coluna **Identificador**.

iii) Acima da grelha de resultados, no campo ao lado do botão de **Filtrar Membros**, você pode filtrar a lista exibida na grelha de resultados ao inserir um dos seguintes itens para um dispositivo:

- **Identificador**, que é um número de série eletrônico atribuído ao agente instalado em cada dispositivo que você selecionou.
- **Nome de Dispositivo**, que é o nome dado a um dispositivo.
- **Nome de usuário**, que é um nome único detectado pelo agente para identificar uma pessoa associada a um dispositivo ou que esteja usando o dispositivo.
- **Número de Série**, que é o número de série do dispositivo.

Clique em **Filtrar Membros** e a grelha de resultados se atualiza e exibe uma lista de dispositivos baseado na sua seleção de filtro.

- Para adicionar dispositivos ao grupo ao especificar dispositivos em um arquivo de texto manualmente, clique em **Carregar uma lista de dispositivos**.

IMPORTANTE Números de série Lenovo com sete caracteres podem ser associados com mais de um dispositivo e pode causar erros quando você carrega uma lista de dispositivos usando um arquivo de texto. Quando você carrega uma lista de dispositivos Lenovo, use números de série completos ou os **Identificadores** de dispositivo Computrace, ambos os quais são únicos para cada dispositivo gerenciado.

i) No diálogo Carregar Lista de Dispositivos para Grupo de Dispositivos, sob a área **Carregar Listas de Números de Série ou Identificadores**, no campo **Caminho do Arquivo**, clique em **Navegar** e procure a localização do arquivo que você deseja carregar.

É possível inserir uma lista de dispositivos em uma única coluna, separando cada entrada com uma linha nova (pressione `Enter`). Não utilize pontuação. Clique **Abrir** para selecionar este caminho de arquivo.

ii) Na área de **Tipo de Lista de Arquivos**, clique em uma das seguintes opções:

- **Números de Série**
- **Identificadores**

iii) Clique em **Carregar Arquivo**. Siga as instruções fornecidas na tela para continuar com este procedimento.

Os dispositivos são adicionados ao grupo de dispositivos.

Adicionando Dispositivos a um Grupo de Dispositivos Automaticamente com base em Endereços IP Locais

Usando a Central do Cliente você pode atribuir dispositivos a grupo de dispositivos automaticamente, baseado no endereço IP local de chamadas dos dispositivos. Este recurso é útil se sua rede incluir várias sub-redes, cada uma com um intervalo de endereços IP locais.

As seguintes regras se aplicam:

- Quando um dispositivo fizer uma chamarda para o Centro de Monitoramento e o seu endereço IP estiver dentro do intervalo de IPs especificado para um grupo de dispositivos, ele é atribuído ao grupo de dispositivos associado àquela sub-rede.
- Quando um dispositivo chama a partir de um endereço IP que não faça parte de um intervalo especificado em um grupo de dispositivos, o dispositivo não é atribuído a nenhum grupo.
- Quando um dispositivo já estiver em um grupo de dispositivos e chamar a partir de um endereço IP que não faça parte daquele ou de qualquer outro grupo de dispositivos, o dispositivo permanecerá no grupo de dispositivos original.
- Quando um dispositivo já está em um grupo de dispositivos e chamar a partir de um endereço IP que faz parte de outro grupo de dispositivos definido, o dispositivo é reatribuído a esse grupo de dispositivos associado a essa sub-rede.

Exemplo

Um distrito escolar está usando a tecnologia Computrace. As seguintes regras de auto-agrupamento estão definidas para duas escolas secundárias no distrito:

- **Auto-agrupamento da Lincoln High School:** Sub-rede local de IPs 172.165.50.*
- **Auto-agrupamento da Washington High School:** Sub-rede local de IPs 172.165.60.*

Se o computador de um professor chamar com o IP **172.165.50.25**, o computador é atribuído automaticamente ao grupo **Lincoln High School**. O professor então leva o computador para casa no fim de semana e o computador chama da casa do professor com o IP **123.134.75.13**. Não existe nenhuma regra de auto-agrupamento para aquela sub-rede de IPs, então o computador permanece no grupo de Lincoln High School.

No entanto, se o professor levar o computador para a **Washington High School** durante alguns dias e chamar a partir de **172.165.60.150**, o computador perde a atribuição à Lincoln High School e fica atribuído ao grupo da Washington High School. Ao contrário do endereço IP da casa do professor, há um auto-agrupamento configurado para aquele IP (Washington High School), e por isso o computador é transferido.

Para usar o recurso de auto-agrupamento da Central do Cliente para adicionar dispositivos a um grupo de dispositivos automaticamente:

1. Crie um arquivo CSV (comma separated value) ou planilha da seguinte forma:
   a) A primeira linha deve ser os cabeçalhos das colunas de **NomeDoGrupo** e **SubRedeIP**.
   b) Linhas subsequentes devem incluir os “<nomes dos grupos de dispositivos>” que você desejar usar, uma vírgula (,) como separador e a SubRedeIP local associada.
   Use o asterisco (*) como caractere curinga para agrupar dispositivos que estão chamando de sub-redes locais diferentes, como demonstrado no seguinte exemplo:
   ```
   NomeDoGrupo,SubRedeIP
   "Nome de Grupo do Dispositivo 1",192.168.*.*
   "Nome de Grupo do Dispositivo 2",172.16.*.*
   "Nome de Grupo do Dispositivo 3",10.*.*.*
   ```
   c) Escolha a opção apropriada para salvar o arquivo em seu dispositivo local.
2. Carregue o arquivo CSV preparado na etapa anterior para a Central do Cliente da seguinte forma:
   a) Entre na Central do Cliente como um Administrador.

b) No painel de navegação, clique em **Administração** > **Grupos** > **Importar Grupo <-> Mapeamento de IP**.

As instruções da tela fornecem tanto orientação sobre a criação de uma planilha e um arquivo de amostra que você pode ver. Você criou este arquivo na etapa 1.

c) No campo **Nome**, digite um nome apropriado para sua importação. Esse nome é usado para rastrear o status da importação do arquivo CSV.

d) Caso deseje receber uma notificação de e-mail quando o processamento da importação estiver concluído, digite seu endereço de e-mail no campo **E-mail**.

e) No campo **Nome do arquivo**, clique em **Navegar** para abrir o diálogo Escolher Arquivo para Carregar e complete as seguintes etapas:

i) Navegue para a local onde você salvou o arquivo CSV editado anteriormente na etapa 1.

ii) Clique no arquivo que deseja carregar e depois clique em **Abrir** para selecionar o arquivo.

A página Importar Grupos é aberta e mostra o caminho para o arquivo selecionado no campo **Nome do Arquivo**. Clique em **Carregar**.

NOTA As importações de arquivos CSV são enfileiradas e processadas em segundo plano. É possível rastrear o progresso de sua importação usando a página Importar Grupo <-> Status de Mapeamento de IP, descrita a seguir.

3. Verifique que o arquivo CSV foi importado com sucesso:

a) No painel de navegação, clique no link **Importar Grupo <-> Status de Mapeamento de IP**.

b) Na página Importar Grupo <-> Status de Mapeamento de IP, na tabela, faça uma revisão ao **Status** de importação.

Quando o processo de importação estiver concluído, o status exibe **Pronto**. Se você forneceu um endereço de email, uma notificação será enviada.

c) Verifique se a importação foi bem sucedida clicando no link **Pronto** e visualizando o status do arquivo CSV.

O arquivo CSV do status é idêntico ao do arquivo CSV que você carregou, com a adição de duas colunas que indicam o sucesso da importação linha a linha.

NOTA Para mais informações, consulte a *Nota Técnica 050221 – Grupo Dinâmico para Mapeamento de Sub-rede de IPs* na página Documentação da Central do Cliente.

Usando Carregamentos em Massa para Alterar as Associações a Grupos de Dispositivos

Manipulando associações de grupo de dispositivos com grandes números de dispositivos pode ser um processo árduo. Para tornar as coisas mais fáceis e rápidas, você pode extrair informações da Central do Cliente, manipulá-las e depois carregar as alterações de volta para a Central do Cliente.

É possível associar cada dispositivo com até 20 grupos de dispositivos diferentes, da seguinte maneira:

- Baixe um arquivo CSV de dispositivos e suas associações atuais ao Grupo do Dispositivos.
- Edite o arquivo CSV para atualizar as associações do grupo de dispositivos. É possível remover qualquer dispositivo cujas associações a grupos não estão se alterando.
- Carregue o arquivo CSV para a Central do Cliente, o que atualizará as associações do grupo de dispositivos.

Para extrair, editar e carregar associações de grupos de dispositivos:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Grupos** > **Exportar Grupos**.
3. Solicite um download de dispositivos em um grupo de dispositivos atual, da seguinte forma:
   a) No local de Critérios de Pesquisa, no campo **O Grupo é**, abra a lista e selecione o grupo de dispositivos apropriado.

   IMPORTANTE Certifique-se de que o download inclui todos os dispositivos que você pretende manipular. Após ter extraído as informações, você não pode adicionar mais dispositivos ao arquivo CSV exportado. Se necessário, baixando o grupo de Todos os Dispositivos garante que você tem todos os dispositivos gerenciados no arquivo CSV.

   b) No local de Nome e Formato, faço o seguinte:
      i) No campo **Nome**, digite um nome apropriado. Este nome aparece na página Status de Exportar Grupo.
      ii) Abra a lista de **Formato** e selecione **CSV** porque só é possível importar um arquivo CSV.

   c) Na área de **Criar Alerta de E-mail**, se você deseja receber uma notificação por e-mail quando o arquivo estiver disponível, insira seu endereço de e-mail no campo **Seu Endereço de E-mail**.
   d) Clique em **Continuar**, o que atualizará a página Exportar Grupos que fornece informações sobre a notificação de quando o relatório estiver pronto.
4. Recupere o arquivo CSV baixado que você acabou de solicitar da seguinte forma:
   a) No painel de navegação, clique no link para **Status de Exportação de Grupos**.

   Se você inseriu um endereço de e-mail na etapa anterior, você pode também clicar no link na mensagem que recebeu.

   b) Quando sua solicitação estiver processada, na tabela, na coluna de **Status**, clique no link de **Pronto** apropriado.
   c) Siga as instruções da tela para **Abrir** o arquivo CSV. Se solicitado, escolha a opção para **Salvar** o arquivo para seu dispositivo local.

   IMPORTANTE É possível abrir o arquivo CSV com praticamente qualquer programa de edição de texto. Entretanto, a Absolute Software recomenda editar o arquivo com um editor de planilhas para preservar o layout de tabelas. Se o layout do arquivo não for preservado, o processo de importação falhará.

   d) Edite o arquivo CSV extraído, da seguinte maneira:

   IMPORTANTE Não altere o formato do arquivo CSV. Alterando o formato fará com que o processo de importação de dados falhe.

   - As primeiras colunas para cada linha contêm o **Identificador**, o **Nome de usuário**, a **Marca** e o **Modelo** do dispositivo.
   - Use estas colunas somente como objetivos de identificação. **Não as edite.**

- As colunas intituladas **Grupo1** a **Grupo20** contêm as associações de grupo que você pode editar. Insira nomes precisos de grupos (sensível às maiúsculas e minúsculas e a ortografia correta) para *associar* o dispositivo com um grupo de dispositivos. É possível *desassociar* um dispositivo de um grupo de dispositivos ao remover o valor.
- É possível remover linhas de dispositivos que você não está editando.
- Não é possível adicionar linhas para dispositivos no arquivo CSV.

e) Salve o arquivo CSV editado no local desejado.

IMPORTANTE A Absolute Software recomenda que você arquive uma cópia do arquivo de download original. Caso ocorra um erro durante o processo de importação, você pode usar o arquivo CSV para restaurar os dados para o estado original.

5. Carregue o arquivo CSV editado da seguinte maneira:

a) Na página Grupos, clique no link **Importar Grupos** para abrir a página Importar Grupos.

b) No campo **Nome**, digite um nome para seu arquivo de importação. Esse nome é usado para rastrear o status da importação do arquivo CSV.

NOTA As importações de arquivos CSV são enfileiradas e processadas em segundo plano. É possível rastrear o progresso de sua importação a partir da página **Status de Importar Grupos**.

c) Caso deseje receber uma notificação de e-mail quando o processamento da importação estiver concluído, digite seu endereço de e-mail no campo **E-mail**.

d) No campo **Nome do arquivo**, clique em **Navegar** para abrir o diálogo Escolher Arquivo para Carregar e complete as seguintes etapas:

i) Navegue para a local onde você salvou o arquivo CSV editado.

ii) Clique no arquivo que deseja carregar e depois clique em **Abrir** para selecioná-lo.

A página Importar Grupos mostra o caminho para o arquivo selecionado no campo **Nome do Arquivo**.

e) Para especificar se vai reter ou remover associação de grupo existentes, selecione uma das seguintes opções:

- **NÃO Exclua a Associação do Grupo Identificador se o Grupo Não Estiver Incluído na Importação** retém as configurações existentes da associação de grupo mesmo que as associações de grupo de dispositivos sejam removidas do arquivo importado. Após o processo de importação ser concluído, quaisquer novos grupos de dispositivos no arquivo importado serão associados ao dispositivo.
- **Excluir a Associação do Grupo Identificador se o Grupo Não Estiver Incluído na Importação**remove associações existentes do grupo, se não estiverem incluídas no arquivo importado. Após o processo de importação ser concluído, o dispositivo estará associado apenas aos grupos de dispositivos especificados no arquivo importado.

f) Clique em **Carregar** para iniciar o processo de importação de arquivo. A página Importar Grupos se atualiza e fornece informações de que seu arquivo foi carregado com sucesso. O arquivo é enfileirado para processamento.

6. Verifique que o arquivo CSV foi processado com sucesso:

a) No painel de navegação, clique no link para **Status de Importação de Grupos**.

b) Na página Status de Importação de Grupos na tabela, faça uma revisão ao **Status** de importação.

Quando concluído, o status exibe **Pronto**. Se você forneceu um endereço de email, uma notificação será enviada.

c) Para verificar o sucesso da importação, clique no link **Pronto** para abrir um arquivo CSV que relata o sucesso ou fracasso de processamento por dispositivo.

Este arquivo é idêntico ao arquivo CSV que você carregou, com a adição de duas colunas que indicam o sucesso ou fracasso da importação linha a linha.

Visualizando os Dispositivos em um Grupo de Dispositivos

Para visualizar os dispositivos em um grupo de dispositivos:

1. Conecte-se à Central do Cliente como um administrador e complete a tarefa, "Visualizando um Grupo de Dispositivos Específico" na página 82.
2. Na página Grupos de Dispositivos, veja a grelha de resultados, que mostra todos os grupos de dispositivos.
3. Para ver que dispositivos estão em um grupo de dispositivos particular, clique no link do nome do grupo de dispositivos desejado, o que abrirá a página Criar e Editar Grupo de Dispositivos.
4. Veja a grelha de resultados, onde você encontrará uma lista de todos os dispositivos que atribuiu a este grupo de dispositivos.
5. Se você desejar rever os detalhes para um dispositivo em particular, clique no link de **Identificador**. Para mais informações, consulte "Editando Informações de Ativos" na página 141.

É também possível usar o Relatório de Ativos para ver os dispositivos dentro de um grupo. Para mais informações, consulte "Relatório de Ativos" na página 153.

Removendo Dispositivos de um Grupo de Dispositivos

Para remover qualquer ou todos os dispositivos de um grupo de dispositivos:

1. Entre na Central do Cliente como um administrador e abra a página Grupos de Dispositivos. Consulte "Visualizando Todos os Grupos de Dispositivos" na página 81.
2. Na página Grupos de Dispositivos, use um dos seguintes métodos para abrir a página Criar e Editar Grupo de Dispositivos com os detalhes do grupo de dispositivos que você deseja editar:
   - Filtre a grelha de resultados para mostrar o grupo de dispositivos particular que você deseja remover. Consulte "Visualizando um Grupo de Dispositivos Específico" na página 82.
   - Na grelha de resultados, clique no link **Nome de Grupo do Dispositivo** para o dispositivo que você deseja excluir.
3. Na página Criar e Editar Grupos de Dispositivos, use uma das seguintes formas de selecionar o dispositivo ou dispositivos que você deseja remover:
   - A partir da coluna **Selecionar tudo**, marque a caixa de seleção para cada dispositivo que você deseja remover do grupo de dispositivos.
   - Marque a caixa de seleção na linha de cabeçalhos da coluna de **Selecionar tudo** para selecionar todos os dispositivos que aparecem na grelha de resultados.
4. Clique em **Remover Dispositivo(s) Selecionado(s)**.

A página Criar e Editar Grupo de Dispositivos é atualizada com uma mensagem de confirmação que fornece os **Identificadores** para cada dispositivo que você removeu.

Excluindo Grupos de Dispositivos

Para excluir um grupo de dispositivos:

1. Conecte-se à Central do Cliente como um administrador e complete a tarefa, "Visualizando Todos os Grupos de Dispositivos" na página 81.
2. Na página Grupos de Dispositivos, na grelha de resultados, clique no link **Nome de Grupo do Dispositivo** para o grupo de dispositivos que você deseja excluir.
3. Na página Criar e Editar Grupo de Dispositivos, clique em **Excluir Este Grupo**.

   Um diálogo de confirmação se abre, avisando que todas as associações ao grupo de dispositivos também serão excluídas. Isto significa que o grupo não será mais exibido em filtros de relatórios e quaisquer alertas aplicados ao grupo de dispositivos não funcionarão mais.
4. Clique em **Excluir este Grupo**. O grupo de dispositivos é excluído.

Política de Software

As políticas de software permitem que Administradores possam definir as regras de software de sua empresa. Uma Política de Software é uma lista de títulos de software Banidos e Obrigatórios. As políticas de software são aplicadas a grupos de dispositivos, após qual dispositivos não conformes são identificados usando o Relatório da Não Conformidade com a Política de Software.

Cada Grupo de Dispositivos pode ser alvo somente de uma política de software. Como um único dispositivo pode pertencer a vários grupos de dispositivos, é possível que um dispositivo seja alvo de várias políticas de software. Neste tipo de cenário, o relatório de Não Conformidade com Políticas de Software mostra quaisquer ocorrências de não conformidade.

Esta seção descreve as seguintes tarefas:

- Visualizar a lista de Políticas de Software
- Visualizando Grupos de Dispositivos sem uma Política de Software
- Criando uma Política de Software
- Criando uma Política de Software ao Copiar uma já existente
- Visualizando uma Política de Software
- Editando uma Política de Software e suas Associações a Grupos de Dispositivos
- Excluindo uma Política de Software

Visualizar a lista de Políticas de Software

Para visualizar as políticas de software que se aplicam a grupos de dispositivos:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Política de Software** > **Ver e Gerenciar Políticas de Software**.
3. Na página Ver e Gerenciar Políticas de Software, a grelha de resultados exibe a seguinte informação sobre suas políticas de software existentes:

- **Nome de Política** é o nome da política.
- **Criado por** é o nome de usuário da pessoa que criou a política.
- **Criado em** é a data e hora quando a política foi originalmente criada.
- **Última atualização por** é o nome de usuário da última pessoa que editou a política.
- **Última atualização em** é a data e hora quando a política foi originalmente editada.
- **Contagem de Grupo** indica o número de grupos de dispositivos a qual se aplica esta política. Clique no link para abrir o diálogo de Grupos de Dispositivos Adicionados a <Nome da Política>.
- O link **Editar** abre a página Criar e Editar uma Política de Software para cada política.

4. Clique em **OK** para fechar o diálogo e voltar a Ver e Gerenciar Políticas de Software.

Visualizando Grupos de Dispositivos sem uma Política de Software

Para visualizar uma lista de grupos de dispositivos que não possuam uma política de software:

1. Complete a tarefa, "Visualizar a lista de Políticas de Software" na página 91.
2. Clique em **Visualizar Grupos sem uma Política**, que abrirá a Política de Software: O diálogo de Grupos sem uma Políticas.
3. A tabela mostra aqueles grupos de dispositivos que não possuam políticas de software aplicados a eles e o **Número de Dispositivos** esta situação afeta.
4. Clique em **Imprimir** para imprimir a lista.

Agora você pode atribuir uma política de software aos grupos de dispositivos apropriados, conforme instruído em um dos seguintes locais:

- Para criar uma nova política de software e aplicá-la a um grupo de dispositivos sem uma política, complete a tarefa, "Criando uma Política de Software" na página 92.
- Para aplicar uma política de software existente a um grupo de dispositivos sem uma política, complete a tarefa, "Editando uma Política de Software e suas Associações a Grupos de Dispositivos" na página 94.

Criando uma Política de Software

Para criar uma política de software:

1. Complete a tarefa, "Visualizar a lista de Políticas de Software" na página 91.
2. Na página Visualizar e Gerenciar Políticas de Software, clique em **Criar Política de Software**, que abre a página Criar e Editar uma Política de Software.

   NOTA No painel de navegação, clicando no link **Criar e Editar Política de Software** também abre a página Criar e Editar uma Política de Software.

3. No campo do **Nome da Política** , digite um nome descritivo para a política.
4. No campo **Descrição**, digite uma breve descrição da política.
5. No lado direito do campo **Grupos de Políticas**, clique em**Adicionar** para abrir o diálogo Escolher Grupos para a Política de Software.
6. Na lista de **Disponíveis**, selecione os grupos de dispositivos apropriados, da seguinte forma:

NOTA No campo **Filtros**, digite os critérios que você deseja usar para filtrar a lista de **Disponíveis** e clique em **Mostrar Resultados**.

- Clique nos grupos de dispositivos que você deseja incluir na política de software e clique em **>** para mover um grupo de dispositivos individual para a lista **Selecionada**.
- Clique em **>>** para mover todos os grupos de dispositivos disponíveis para a lista de **Selecionados**.
- Clique em **Todos os Dispositivos** para selecionar todos os grupo de dispositivos.

  NOTA Se, por engano, você mover um grupo de dispositivos disponível para a lista de **Selecionadas**, poderá selecionar o grupo de dispositivos e clicar em **<** para movê-lo de volta para a lista de **Disponíveis**.

- Ao concluir, clique em **OK**.

  A página Criar e Editar uma Política de Software se atualiza com uma lista atualizada dos grupos de dispositivos selecionados no campo **Grupos de Políticas**, baseado em suas seleções.

7. Defina os **Itens Banidos** para a Política de Software da seguinte forma:

   a) Clique no separador de **Itens Banidos** e depois clique em **Adicionar**.

   No diálogo Escolher Licenças de Software ou Programas Executáveis, a lista mostra por padrão todos os Fornecedores e Aplicativos disponíveis. É possível usar o filtro para pesquisar no banco de dados para reduzir a lista, o que facilitará a localização do aplicativo que você deseja.

   b) Para filtrar a lista, faça o seguinte:

   i) No campo **Filtro** digite parte ou todo o nome de um **Fornecedor** ou **Aplicativo**.

   ii) Selecione a opção apropriada para exibir licenças e/ou executáveis:

   - **Mostrar Apenas Licenças**
   - **Mostrar Apenas Programas Executáveis**
   - **Exibir tanto as Licenças como os Programas Executáveis (recomendado)**
   - **Mostrar Licenças/Executáveis com Versões Independentes**
   - **Mostrar Licenças/Executáveis com Versões Específicas**

   iii) Para ver somente as licenças instaladas nos dispositivos de sua empresa, marque a caixa de seleção **Exibir Somente Licenças ou Programas Executáveis Instalados nos Dispositivos da sua Empresa**.

   iv) Clique em **Filtrar**.

   c) Adicionar um ou mais aplicativos à **Listas de Proibidos**:

   i) Sob a coluna **Editores**, clique em um nome específico para mostrar todos os aplicativos para aquele editor na coluna **Aplicativos**.

   ii) Selecione aplicativos para adicionar da seguinte forma:

   - Para selecionar um aplicativo, clique em um nome de um **Aplicativo** e clique em **>** para mover um aplicativo individual para a lista de **Selecionados**.
   - Para selecionar todos os aplicativos de um editor, clique em **>>** para mover todos os aplicativos disponíveis para a lista de **Selecionados**.
   - Para remover um aplicativo da lista de **Selecionados**, clique no nome naquela lista e em seguida clique **<** para movê-lo para a lista de **Aplicativos**.

- Para remover todos os aplicativos da lista de **Selecionados**, clique em **<<** para movê-los todos para a lista de **Aplicativos**.

iii) Clique em **OK**.

8. Defina os **Itens Obrigatórios** para a política de software da seguinte forma:

   a) Clique no separador de **Itens Obrigatórios** e em seguida clique em **Adicionar**, que abrirá o diálogo de Escolher Licenças de Software ou Programas Executáveis.

   b) O processo de filtragem da lista e da adição de aplicativos à lista de **Itens Obrigatórios** é idêntico ao processo descrito para a lista de **Itens Proibidos**. Para mais informações, consulte etapa 7.

9. Salve a Política de Software fazendo uma das seguintes ações:

   - Clique em **Salvar e Fechar** para salvar as alterações e ir para a página Visualizar e Gerenciar Políticas de Software.
   - Clique em **Salvar** para salvar as alterações e atualizar a página Criar e Editar a Política de Software.

Criando uma Política de Software ao Copiar uma já existente

Para criar uma Política de Software copiando uma já existente:

1. Para a política de software de qual você pretende copiar, complete a tarefa, "Visualizando uma Política de Software" na página 94.
2. Na página Criar e Editar Política de Software, clique em **Copiar** para criar uma nova política de software.

   A página Criar e Editar Políticas de Software se atualiza, mostrando a nova política. As palavras "Cópia de" são acrescentadas ao nome da política de software copiada.

3. Edite a Política de Software como achar apropriado. Consulte "Editando uma Política de Software e suas Associações a Grupos de Dispositivos" na página 94.

Visualizando uma Política de Software

Para visualizar uma política de software:

1. Complete a tarefa, "Visualizar a lista de Políticas de Software" na página 91.
2. Encontre o **Nome de Política** da política que você deseja ver e clique no link de **Editar** correspondente.

Editando uma Política de Software e suas Associações a Grupos de Dispositivos

Para editar uma política de software já existente e seus grupos de dispositivos associados:

1. Complete a tarefa, "Visualizando uma Política de Software" na página 94.
2. Na página Criar e Editar Políticas de Software, edite a Política de Software da seguinte forma:

   - No campo do **Nome de Política**, edite o nome existente conforme apropriado.
   - No campo da **Descrição da Política**, edite a descrição conforme apropriado.

3. Para adicionar mais grupos de dispositivos à política de software, faça o seguinte:
   a) No campo **Grupos de Políticas**, você pode adicionar esta política a mais grupos ao clicar em **Adicionar**.
   b) No diálogo de Escolher Grupos para a Política de Software, certifique-se de que os grupos de dispositivos apropriados são movidos da lista de **Disponíveis** à lista de **Selecionados**.
   c) Clique em **OK** para fazer as alterações aos **Grupos de Políticas**.
4. Para remover um grupo de dispositivos desta política de software, no campo **Grupos de Políticas**, selecione o grupo de dispositivos apropriado e clique em **Remover**.
5. Para adicionar ou remover produtos de software da lista de software de **Itens Proibidos** e de **Itens Obrigatórios**, siga as instruções fornecidas na etapa 7 da tarefa, "Criando uma Política de Software" na página 92.
6. Faça uma das seguintes opções:
   - Clique **Salvar e Fechar** para salvar suas alterações, e voltar à página de Visualizar e Gerenciar Políticas de Software.
   - Clique em **Salvar** para salvar as alterações e permanecer na página atualizada de Criar e Editar a Política de Software.
   - Para exportar a informação desta política de software para uma planilha, clique em **Exportar para Excel**. Faça uma das seguintes opções:
     - Clique em **Abrir** para mostrar o conteúdo desta política de software em Microsoft Excel.
     - Clique em **Salvar** para salvar a planilha e abri-la mais tarde.

Excluindo uma Política de Software

Para excluir uma política de software:

1. Complete a tarefa, "Visualizando uma Política de Software" na página 94.
2. Na página Criar e Editar Políticas de Software, clique em **Excluir**.

IMPORTANTE **Aja com cautela**. Quando você clica em **Excluir**, a política é excluída sem pedir confirmação de sua parte.

Usuários

A seção de Usuários é onde você cria usuários da Central do Cliente e indica seus direitos de acesso e suas restrições. Os recursos de segurança multi-nível da Central do Cliente possibilitam que um usuário autorizado (um administrador) conceda diferentes direitos e privilégios a usuários ou grupos de usuários específicos.

A Central do Cliente fornece as seguintes funções de usuário:

- Os **Administradores** são aqueles usuários que gerenciam os dispositivos e ativos de TI de suas empresas, relatam a perda ou o furto de dispositivos, e criam e gerenciam várias comunicações de sistema, tais como mensagens do usuário final, notificações do sistema e alertas e eventos de alertas suspeitos.

- Os **administradores de segurança** existem naquelas empresas que decidem designar certos administradores como administradores de segurança para gerenciar a segurança de dispositivos e de dados de ativos gerenciados. Esta função de usuário tem mais direitos de acesso que a função do Administrador.

  Os Administrador de Segurança possuem a autoridade para configurar, selecionar e iniciar serviços de Recuperação de Arquivos, de Congelamento de Dispositivo e de Exclusão de Dados. Os administradores de segurança usam a Central do Cliente para rastrear e gerenciar dispositivos, tanto dentro como fora da rede local da empresa.
- **Usuários Avançados** têm direitos de acesso para a maioria de recursos da Central do Cliente, excluindo recursos de segurança. Administradores podem restringir os direitos de Usuários Avançados a identificadores ou grupos de dispositivos específicos.
- **Usuários de Segurança Avançados** existem naquelas empresas que decidem designar certos Usuários Avançados como Usuários de Segurança Avançados para gerenciar a segurança de dispositivos e de dados de ativos. Esta função de usuário possui mais direitos de acesso do que a função do Usuário Avançado.

  Os Usuários de Segurança Avançados possuem a autoridade para configurar, selecionar e iniciar serviços de Recuperação de Arquivos, de Congelamento de Dispositivo e de Exclusão de Dados para dispositivos no Grupo de Dispositivos atribuído a eles. Os Usuários de Segurança Avançados usam a Central do Cliente para rastrear e gerenciar dispositivos dentro da rede local da empresa.
- **Usuários Convidados** têm acesso limitado a informação e a relatórios da Central do Cliente. Estes usuários não podem alterar ou atribuir direitos de acesso a usuários nem podem alterar detalhes na página Resumo do Dispositivo. Membros do Grupo de Convidados só podem navegar pelos Relatórios de Furto que eles mesmos criaram e só podem visualizar Relatórios Salvos que eles mesmos salvaram.

Para informações detalhadas sobre cada função de usuário e seus direitos de acesso aos recursos e funcionalidades da Central do Cliente, consulte "As Funções de Usuários da Central do Cliente e Seus Direitos de Acesso " na página 97.

Esta seção fornece informações sobre os seguintes tópicos e tarefas:

- Funções de usuário e seus direitos de acesso
- Criar Novos Usuários
- Visualizando os Usuários em Sua Conta
- Editando os Detalhes de um Usuário
- Suspendendo um Usuário
- Ativando um usuário suspenso
- Excluindo Usuários

Funções de usuário e seus direitos de acesso

A seguinte tabela define o nível de acessibilidade de cada função de usuário aos recursos da Central do Cliente.

Estas informações podem diferir da situação específica da sua empresa. Por exemplo, em algumas empresas, a função de usuário do Administrador de Segurança é desempenhada pela função de usuário do Administrador.

As Funções de Usuários da Central do Cliente e Seus Direitos de Acesso

Recursos dos Aplicativos da Central do Cliente	Administrador de Segurança	Administrador	Usuário de Segurança Avançado	Usuário Avançado	Convidado
Área de **Relatórios**					
Pode visualizar todos os relatórios?	Sim	Sim	Sim	Sim	Yes, com uma exceção[a]
Pode visualizar todos os dispositivos na conta?	Sim	Sim	Não, a visualização pode ser restringida a um grupo de dispositivos quando você criar este usuário	Não, a visualização pode ser restringida a um grupo de dispositivos quando você criar este usuário	Não, a visualização pode ser restringida a um grupo de dispositivos quando você criar este usuário
Quais as funções no Resumo de Dispositivos que estão disponíveis para este usuário?	Visualizar e editar	Visualizar e editar	Visualizar e Editar baseado em restrições de grupos de dispositivos	Visualizar e Editar baseado em restrições de grupos de dispositivos	Somente visualizar
Pode visualizar todos os seus relatórios salvos (Meus Relatórios)? (Não pode ver os relatórios salvos de outros usuários).	Sim	Sim	Sim	Sim	Sim
Área de**Administração**					
Pode acessar a seção de **Alertas**?	Sim	Sim	Sim	Sim	Sim
Pode abrir e visualizar **Eventos de Alertas**?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos

[a] Os usuários convidados não podem acessar a área de Gerenciamento de Contas e, portanto, não podem ver quaisquer relatórios aí contidos. Adicionalmente, estes usuários não podem ver o Relatório de Dispositivos Suspeitos, o Relatório de Localização do Dispositivo ou o Relatório de Histórico da Localização do Dispositivo.

As Funções de Usuários da Central do Cliente e Seus Direitos de Acesso (continuado)

Recursos dos Aplicativos da Central do Cliente	Administrador de Segurança	Administrador	Usuário de Segurança Avançado	Usuário Avançado	Convidado
Pode criar e editar **Alertas** e suspender a verificação de alertas?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos
Pode abrir e visualizar **Alertas**?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos
Pode excluir **Alertas**?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos
Pode acessar a seção de **Dados**?	Sim	Sim	Sim	Sim	Sim
Pode criar, editar e excluir departamentos?	Sim	Sim	Sim	Sim	Não, apenas visualizar
Pode exportar dados e visualizar o status da exportação de dados?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos
Pode importar dados e visualizar o status da importação de dados?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos
Pode acessar arquivos importados?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos

As Funções de Usuários da Central do Cliente e Seus Direitos de Acesso (continuado)

Recursos dos Aplicativos da Central do Cliente	Administrador de Segurança	Administrador	Usuário de Segurança Avançado	Usuário Avançado	Convidado
Pode criar e editar campos definidos pelo usuário?	Sim	Sim	Não	Não	Não
Pode visualizar e editar os valores de dados de campos definidos pelo usuário?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não, apenas visualizar
Pode criar, editar e excluir mensagens de usuários finais?	Sim	Sim	Não	Não	Não
Pode acessar a seção de **Cercas Geográficas**?	Sim	Sim	Sim	Sim	Não
Pode criar e editar cercas geográficas?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não
Pode visualizar e gerenciar cercas geográficas?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não
Pode acessar a seção de **Grupos**?	Sim	Sim	Sim	Sim	Sim
Pode visualizar grupos de dispositivos?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos
Pode criar, editar e excluir grupos de dispositivos?	Sim	Sim	Não	Não	Não

As Funções de Usuários da Central do Cliente e Seus Direitos de Acesso (continuado)

Recursos dos Aplicativos da Central do Cliente	Administrador de Segurança	Administrador	Usuário de Segurança Avançado	Usuário Avançado	Convidado
Pode adicionar e remover dispositivos a/de grupos de dispositivos?	Sim	Sim	Não	Não	Não
Pode conceder direitos de somente leitura a outros usuários?	Sim	Sim	Não	Não	Não
Pode importar grupos para o mapeamento de IP e visualizar o status resultante?	Sim	Sim	Não	Não	Não
Pode exportar informações de grupo de dispositivos para uma planilha ou arquivo XML e visualizar seu status?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos
Pode importar informações de grupo de dispositivos de uma planilha e visualizar seu status?	Sim	Sim	Não	Não	Não
Pode acessar arquivos importados?	Sim	Sim	Não	Não	Não
Pode acessar a seção **Política de Software**?	Sim	Sim	Não	Não	Não
Pode visualizar grupos com e sem políticas de software?	Sim	Sim	Não	Não	Não
Pode criar, editar e excluir políticas de software?	Sim	Sim	Não	Não	Não

As Funções de Usuários da Central do Cliente e Seus Direitos de Acesso (continuado)

Recursos dos Aplicativos da Central do Cliente	Administrador de Segurança	Administrador	Usuário de Segurança Avançado	Usuário Avançado	Convidado
Pode copiar ou imprimir políticas de software?	Sim	Sim	Não	Não	Não
Pode exportar uma política de software para Excel?	Sim	Sim	Não	Não	Não
Pode acessar a seção **Usuários**?	Sim	Sim	Sim	Sim	Não
Pode visualizar e gerenciar os usuários da sua conta?	Sim	Sim	Sim, ação limitada apenas a usuários convidados para dispositivos atribuídos e grupos de dispositivos	Sim, ação limitada apenas a usuários convidados para dispositivos atribuídos e grupos de dispositivos	Não
Pode criar, editar e excluir usuários?	Sim	Sim	Sim, limitado a usuários convidados	Sim, limitado a usuários convidados	Não
Pode editar e atribuir funções de usuários a outros usuários?	Sim, limitado a usuários avançados e usuários convidados	Sim, limitado a usuários avançados e usuários convidados	Não	Não	Não
Pode editar detalhes de usuário?	Sim	Sim	Sim, limitado a usuários convidados	Sim, limitado a usuários convidados	Não
Pode alterar a **senha** de outros usuários?	Sim	Sim	Sim, limitado a usuários convidados	Sim, limitado a usuários convidados	Não
Pode editar os grupos de dispositivos que são visíveis a outros usuários?	Sim, limitado a usuários avançados e usuários convidados	Sim, limitado a usuários avançados e usuários convidados	Não	Não	Não
Pode editar as **definições de sistema de usuário** de outros usuários?	Sim	Sim	Sim, limitado a usuários convidados	Sim, limitado a usuários convidados	Não

As Funções de Usuários da Central do Cliente e Seus Direitos de Acesso (continuado)

Recursos dos Aplicativos da Central do Cliente	Administrador de Segurança	Administrador	Usuário de Segurança Avançado	Usuário Avançado	Convidado
Pode editar as **configurações de status e de suspensão** de um outro usuário?	Sim	Sim	Sim, limitado a usuários convidados	Sim, limitado a usuários convidados	Não
Pode editar informação no **Meu Perfil**, excluindo as funções de conta, nome de usuário e função de usuário?	Sim	Sim	Sim, com exceções (não pode ver configurações de remoção de agentes e não pode editar quaisquer configurações de auto-suspensão)	Sim, com exceções (não pode ver configurações de remoção de agentes e não pode editar quaisquer configurações de auto-suspensão)	Sim, com exceções (não pode ver configurações de remoção de agentes e não pode editar quaisquer configurações de auto-suspensão)
Pode acessar a seção **Conta**?	Sim	Sim	Sim	Sim	Sim
Pode editar as definições padrão para idioma e localidade, fuso horário e licenças de garantia de serviço?	Sim	Sim	Não, somente leitura	Não, somente leitura	Não, somente leitura
Pode ativar a configuração para começar a coleção de dados de criptografia de discos completos dos dispositivos.	Sim	Sim	Não, apenas visualizar	Não, apenas visualizar	Não, apenas visualizar
Pode **Adicionar Licenças** ao digitar Chaves de Produto?	Sim	Sim	Não, somente leitura	Não, somente leitura	Não, somente leitura
Pode visualizar e baixar os pacotes de instalação de agentes para sua conta?	Sim	Sim	Não	Não	Não
Pode acessar a seção **Notificações de Sistema**?	Sim	Sim	Sim	Sim	Sim, somente leitura

As Funções de Usuários da Central do Cliente e Seus Direitos de Acesso (continuado)

Recursos dos Aplicativos da Central do Cliente	Administrador de Segurança	Administrador	Usuário de Segurança Avançado	Usuário Avançado	Convidado
Pode editar ou remover os endereços de e-mail configurados para receber notificações de sistema?	Sim	Sim	Sim	Sim	Não
Pode acessar a seção **Desativar a Pré-Autorização**?	Sim	Sim	Não	Não	Não
Pode desativar o acordo de autorização para operações de segurança?	Sim	Não	Não	Não	Não
Pode acessar a seção **Criar e Visualizar Solicitações de Remoção de Agentes**?	Estas informações podem diferir da situação específica da sua empresa. Por exemplo, em algumas empresas, as tarefas da função de usuário do Administrador de Segurança são desempenhadas pelo Administrador, caso em que o Administrador possui os direitos de acesso exibidos para o Administrador de Segurança.				
	Sim	Sim, se a Remoção de Agentes estiver ativa no perfil do usuário	Sim, se a Remoção de Agentes estiver ativa no perfil do usuário	Sim, se a Remoção de Agentes estiver ativa no perfil do usuário	Não
Pode ver solicitações de remoção de agentes?	Sim	Sim, se a Remoção de Agentes estiver ativa no perfil do usuário	Sim, se a Remoção de Agentes estiver ativa no perfil do usuário	Sim, se a Remoção de Agentes estiver ativa no perfil do usuário	Não
Pode criar novas solicitações para a remoção de agentes?	Sim	Sim, se a Remoção de Agentes estiver ativa no perfil do usuário	Sim, se a Remoção de Agentes estiver ativa no perfil do usuário	Sim, se a Remoção de Agentes estiver ativa no perfil do usuário	Não
Pode carregar uma lista de dispositivos para múltiplas solicitações de remoção de agentes?	Sim	Sim, se a Remoção de Agentes estiver ativa no perfil do usuário	Sim, se a Remoção de Agentes estiver ativa no perfil do usuário	Sim, se a Remoção de Agentes estiver ativa no perfil do usuário	Não

As Funções de Usuários da Central do Cliente e Seus Direitos de Acesso (continuado)

Recursos dos Aplicativos da Central do Cliente	Administrador de Segurança	Administrador	Usuário de Segurança Avançado	Usuário Avançado	Convidado
Área de **Segurança de Dados e Dispositivos**	Estas informações podem diferir da situação específica da sua empresa. Por exemplo, em algumas empresas, as tarefas da função de usuário do Administrador de Segurança são desempenhadas pelo Administrador, caso em que o Administrador possui os direitos de acesso exibidos para o Administrador de Segurança.				
Pode acessar a seção de **Autorização de Segurança**?	Sim	Sim	Sim	Não	Não
Pode solicitar um token de autorização de segurança e possui a autoridade de solicitar um código de autorização?	Sim	Não	Sim	Não	Não
Pode acessar a seção de **Exclusão de Dados**?	Sim	Sim	Sim	Não	Não
Pode visualizar o Relatório de Resumos de Exclusão de Dados para ver solicitações de Exclusão de Dados ativas?	Sim	Sim, somente leitura	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Pode solicitar uma operação de Exclusão de Dados?	Sim	Não	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Pode visualizar políticas de Exclusão de Dados, datas alteradas e solicitações ativas?	Sim	Sim	Sim	Não	Não
Pode criar, editar, copiar e excluir políticas de Exclusão de Dados?	Sim	Não	Sim	Não	Não

As Funções de Usuários da Central do Cliente e Seus Direitos de Acesso (continuado)

Recursos dos Aplicativos da Central do Cliente	Administrador de Segurança	Administrador	Usuário de Segurança Avançado	Usuário Avançado	Convidado
Pode editar políticas de Exclusão de Dados pré-definidas?	Sim	Não	Sim	Não	Não
Pode acessar a seção de **Congelamento de Dispositivo**?	Sim	Sim	Sim	Sim	Não
Pode visualizar o relatório de resumos de congelamento de dispositivos para ver uma lista de dispositivos que têm solicitações de congelamento de dispositivos pendentes?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não
Pode solicitar uma operação de congelamento de dispositivos e forçar uma reinicialização?	Sim	Não	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Pode visualizar, criar, pré-visualizar, editar e excluir mensagens de congelamento de dispositivos?	Sim	Sim	Sim	Não, apenas pré-visualizar	Não
Pode visualizar, criar, editar e excluir políticas de Congelamento de Dispositivos do estado offline?	Sim	Não	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Pode acessar a seção de **Intel Anti-Theft Technology**?	Sim	Sim	Sim	Sim	Não

As Funções de Usuários da Central do Cliente e Seus Direitos de Acesso (continuado)

Recursos dos Aplicativos da Central do Cliente	Administrador de Segurança	Administrador	Usuário de Segurança Avançado	Usuário Avançado	Convidado
Pode solucionar problemas de desinscrição da Intel AT?	Sim	Não, somente leitura	Não, apenas somente leitura para dispositivos e grupos de dispositivos atribuídos	Não, apenas somente leitura para dispositivos e grupos de dispositivos atribuídos	Não
Pode acessar a seção de **Lista de Arquivos**?	Sim	Sim	Sim	Não	Não
Pode visualizar o Relatório de Resumos de Listas de Arquivos para ver uma lista de solicitações de Listas de Arquivos?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Pode solicitar uma nova lista de arquivos (criar uma solicitação de Listas de Arquivos)?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Pode cancelar uma solicitação de lista de arquivos?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Pode remover a solicitação?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Pode imprimir e salvar a lista de listas de arquivos solicitadas?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Pode acessar a seção de **Recuperação de Arquivos Remota**?	Sim	Não	Sim	Não	Não

As Funções de Usuários da Central do Cliente e Seus Direitos de Acesso (continuado)

Recursos dos Aplicativos da Central do Cliente	Administrador de Segurança	Administrador	Usuário de Segurança Avançado	Usuário Avançado	Convidado
Pode visualizar o Relatório de Resumos de Recuperação de Arquivos para ver uma lista de solicitações de Recuperações de Arquivos Remotas?	Sim	Não	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Pode solicitar uma nova recuperação de arquivos (criar uma solicitação de Recuperação de Arquivos Remota)?	Sim	Não	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Pode cancelar uma solicitação de recuperação de arquivos?	Sim	Não	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Pode remover a solicitação?	Sim	Não	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Pode imprimir e salvar a lista de recuperações de arquivos solicitadas?	Sim	Não	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Não	Não
Área de **Relatório de Furto**					
Pode visualizar o status de relatórios de furto existentes?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos

As Funções de Usuários da Central do Cliente e Seus Direitos de Acesso (continuado)

Recursos dos Aplicativos da Central do Cliente	Administrador de Segurança	Administrador	Usuário de Segurança Avançado	Usuário Avançado	Convidado
Pode criar novos relatórios de furto?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos
Pode atualizar relatórios de furto existentes?	Sim	Sim	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos	Sim, apenas para dispositivos atribuídos e grupos de dispositivos
Pode atualizar a Lista de Contatos de Relatórios de Furto?	Sim	Não, apenas pré-visualizar	Não, apenas pré-visualizar	Não, apenas pré-visualizar	Não
Área de **Documentação**					
Pode abrir e visualizar documentos listados?	Sim	Sim	Sim	Sim	Sim
Área de **Suporte**					
Pode enviar um processo de suporte?	Sim	Sim	Sim	Sim	Sim

Criar Novos Usuários

Antes de criar um novo usuário, você precisa compreender os diferentes direitos de acesso disponíveis a cada um dos grupos de usuários. Consulte "Funções de usuário e seus direitos de acesso" na página 96.

Para criar um novo usuário:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.
2. No painel de navegação, clique **Administração** > **Usuários**>**Criar e Editar Usuário**.
3. Na página Criar e Editar Usuários, na área **Detalhes de Usuário**, forneça as seguintes informações:
   a) No campo **E-mail** , digite o endereço de e-mail que é usado para enviar notificações de e-mail ao usuário.
   b) O campo **Nome de Usuário** é preenchido com aquilo que você acabou de inserir no campo **E-mail**.
   Se você deseja um nome de usuário diferente, clique neste campo, remova o conteúdo e digite o nome de usuário de sua preferência para este usuário.

Este campo requer conteúdo com um mínimo de 6 caracteres.

c) Abra a lista **Função** e selecione uma das seguintes funções:
   - Administrador
   - Usuário Avançado
   - Convidado

NOTA Se você estiver conectado como um usuário avançado, pode selecionar apenas a função de Convidado apenas.

Para mais informações sobre as funções de usuário e seus direitos de acesso associados, consulte "Funções de usuário e seus direitos de acesso" na página 96.

NOTA Para conceder privilégios de autorização de segurança a um Administrador ou Usuário Avançado, consulte "Protegendo seus dados e dispositivos" na página 258.

d) Nos campos de **Primeiro Nome** e **Sobrenome** , digite o primeiro nome e o sobrenome do usuário, respetivamente.

e) No campo **Definir Senha**, digite uma senha, com um mínimo de seis caracteres, para este usuário poder se conectar na Central do Cliente.

f) No campo **Confirmar Senha**, digite a senha novamente.

g) Selecione todas as opções desejadas a partir da seguinte lista:
   - **O usuário deve alterar a Senha no próximo login** obriga o usuário a alterar a senha de login na próxima conexão bem sucedida.
   - **O usuário deve alterar a Senha a cada 30 dias** obriga o usuário a alterar a senha de login a cada 30 dias.
   - **Exigir senha forte** força o usuário a usar apenas senhas fortes. Senhas fortes devem conter no mínimo 8 caracteres e conter uma mistura de caracteres maiúsculos e minúsculos alfanuméricos e/ou símbolos.

h) Se você desejar restringir o acesso do usuário a um dispositivo individual (Identificador) ou a um grupo de dispositivos, selecione um valor a partir da lista de **Grupos de Dispositivos**.

NOTA É possível selecionar apenas um único dispositivo ou grupo de dispositivos para um usuário individual. Se você estiver conectado como um usuário avançado, este campo se associa por padrão ao grupo de dispositivos a que você está atribuído. Pode ser necessário criar um novo grupo de dispositivos para limitar os direitos de monitoramento de um usuário específico. Para mais informações, consulte "Criando um Novo Grupo de Dispositivos" na página 79.

4. Na área **Configurações de Sistema do Usuário**, forneça as seguintes informações:

   a) No campo **Idioma e Localização Padrão do Usuário**, abra a lista e selecione o idioma e local associado.

   b) No campo **Fuso Horário Padrão**, abra a lista e selecione um fuso horário.

   c) No campo **Tempo Limite Padrão da Sessão do Usuário**, abra a lista e selecione um valor.

5. Na área **Configurações de Status e suspensão do Usuário**, forneça as informações desejadas nas seguintes seções:

- **Status do Usuário**: Selecione o status desejado a partir das seguintes opões:
  - **Ativo**: Selecione esta opção para ativar usuários desativados ou suspensos. Esta opção é o valor padrão para usuários novos e existentes.
  - **Suspenso**: Selecione esta opção para manualmente suspender um usuário ativo.
  - **Temporariamente suspenso até**: Selecione esta opção e digite uma data ou clique no calendário para o abrir. No calendário, selecione uma data final para a suspensão.
- **Auto-suspensão por falhas de login**: Selecione a configuração de auto-suspensão desejada a partir das seguintes escolhas:
  - **Nunca auto-suspender usuário por falhas de login:** Selecione esta opção para permitir falhas de login ilimitadas para o usuário.
  - **Auto-suspender usuário após 3 tentativas de login falhadas**: Selecione esta opção para suspender automaticamente um usuário após três tentativas de login falhadas. Esta opção é a configuração padrão para todos os usuários, a menos que seja selecionado especificamente o contrário. Esta opção também requer que o administrador ative o usuário. Para mais informações, consulte "Ativando um usuário suspenso" na página 114.
  - **Auto-suspender temporariamente o usuário por 24 horas após 3 tentativas de login falhadas**: Selecione esta opção para suspender automaticamente um usuário por 24 horas a partir da hora da última tentativa de login falhada, após 3 tentativas de login falhadas.
  - **Enviar e-mail a todos os administradores se um usuário for suspenso devido a inatividade**: Marque esta caixa de seleção para enviar uma notificação por e-mail para todos os administradores da sua conta, sempre que um usuário for suspenso por tentativas de login falhadas.
- **Auto-suspensão por inatividade:** Selecione a configuração de suspensão automática apropriada a partir das seguintes opções:
  - **Nunca auto-suspender por inatividade**: Selecione esta opção para permitir que os usuários se conectem à Central do Cliente após longos períodos de tempo.
  - **Auto-suspender se o usuário não fizer login durante 30 dias:** Selecione esta opção para suspender automaticamente um usuário, se o usuário não tiver se conectado à Central do Cliente durante um período de tempo específico.

6. Se a área **Remoção de Agentes** estiver disponível e você desejar permitir que este usuário faça solicitações de remoção de agentes, marque a caixa de seleção. Para mais informações, consulte "Gerenciando solicitações de remoção de agentes" na página 132.

   Se você é o administrador de segurança, o diálogo Digite Código de Autorização é exibido, solicitando que você forneça autorização. Dependendo de que método de autenticação de segurança sua empresa escolheu, faça uma das seguintes ações:

   - Para empresas que usam Tokens RSA SecurID para serviços de segurança:
     - Digite sua **Senha** da Central do Cliente.
     - Digite o **Código do Token SecurID** que aparece em seu Token RSA SecurID.

     Para mais informações, consulte "Usando Tokens RSA SecurID para Serviços de Segurança" na página 263.
   - Para empresas que usam códigos de autorização enviados por e-mail para serviços de segurança:

- Clique em **Gerar um novo token de autorização enviado por e-mail**. A página se atualiza e fornece confirmação de que uma mensagem de e-mail foi enviada para o endereço registrado para o administrador de segurança que está fazendo a solicitação.
- Digite sua **Senha da Central do Cliente**.
- Digite o **Código de Autorização** de Segurança que você recebeu na mensagem de e-mail.

Para mais informações, consulte "Usando Códigos de Autorização Enviados por E-mail para Serviços de Segurança" na página 264.

7. Depois de inserir todas as informações para o novo usuário, clique em **Salvar**.

   A página Visualizar e Gerenciar Usuários se abre e exibe uma mensagem informando que o novo usuário foi criado com sucesso e os seus detalhes estão na grelha de resultados.

Visualizando os Usuários em Sua Conta

Quando você tiver criado os vários usuários em sua conta, pode ver uma tabela que fornece uma lista dos três grupos de usuários e os usuários atribuídos a cada grupo.

Para visualizar os usuário em sua conta:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Usuários** > link para **Ver e Gerenciar Usuários**.

   Na página Ver e Gerenciar Usuários, a grelha de resultados mostra todas as funções de usuário e os usuários atribuídos a cada função. Se você não conseguir ver os usuários atribuídos inicialmente, expanda o nome da função de usuário para exibi-los Pode ser necessário rolar pelas páginas da lista para ver todos os usuários.

Editando os Detalhes de um Usuário

Para editar informações para um usuário existente:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.
2. No painel de navegação, clique em **Administração** > **Usuários** > **Ver e Gerenciar Usuários**.
3. Na página Ver e Gerenciar Usuários, role pela lista de usuários e quando você encontrar os usuários cujos detalhes deseja editar, clique no link **Editar** no lado extremo direito dessa linha.

   NOTA Se você estiver conectado como um usuário avançado, pode editar apenas os usuários Convidados.

4. Na página Gerenciar Detalhes do Usuário, edite as informações apropriadas para o usuário da seguinte forma:

   NOTA Se você precisa de uma explicação para qualquer um dos campos, consulte a etapa 3 a etapa 7 da tarefa, "Criar Novos Usuários" na página 108.

   a) No campo **E-mail**, digite o endereço de e-mail para este usuário. O campo de **Nome de Usuário** pode ser preenchida com esta mesma informação.

NOTA Alterando o endereço de e-mail de uma administrador de segurança ou usuário de segurança avançado suspende temporariamente a capacidade do usuário para executar operações de segurança durante as próximas 72 horas. Para mais informações, consulte "Usando Códigos de Autorização Enviados por E-mail para Serviços de Segurança" na página 264.

b) Se você estiver conectado como um administrador, clique no campo **Função** e selecione uma função da lista.

IMPORTANTE Administradores podem alterar a **Função** de usuário de Usuários Avançados e de Convidados. Eles não podem alterar a **Função** de outros Administradores, Administradores de Segurança e Usuários de Segurança Avançados.

NOTA Para usuários que são designados como administradores de segurança, o seguinte texto é exibido acima do campo de **Função**:
O Usuário está registrado como Administrador de Segurança. A função pode ser alterada apenas ao contatar o Suporte Técnico.
Um texto semelhante é exibido para Usuários de Segurança Avançados.

c) No campo **Primeiro Nome**, digite o primeiro nome apropriado.

d) No campo **Sobrenome**, digite o sobrenome apropriado.

e) Na área com as caixas de seleção, clique nas opções apropriadas para este usuário a partir da seguinte lista:

- **O usuário deve mudar a senha no próximo login**
- **O usuário deve mudar a senha a cada 30 dias**
- **Exigir senha forte**

  Se uma senha forte for necessária, a nova senha deve conter no mínimo 8 caracteres e conter uma mistura de caracteres maiúsculos e minúsculos alfanuméricos e/ou símbolos.

f) Na parte inferior da área **Detalhes do usuário**, sob **Senha**, clique no link **Alterar Senha**.

No diálogo Alterar Senha, faça o seguinte:

i) No campo **Definir Nova Senha** digite uma nova senha.

ii) No campo **Confirmar Nova Senha**, digite a nova senha novamente.

iii) Clique em **Salvar**. O diálogo de Alterar Senha se atualiza e exibe uma mensagem confirmando as alterações que você fez.

iv) Clique em **Continuar** para voltar à página Gerenciar Perfil de Usuário.

v) No campo **Grupo de Dispositivos**, abra a lista e selecione o grupo de dispositivos desejado.

g) Na área **Configurações de sistema do usuário**, abra as listas e selecionar os valores apropriados para o seguinte:

- No campo **Idioma e Localização do Usuário Padrão**, abra a lista e selecione as informações apropriadas.

  NOTA Se você selecionar um novo valor para o campo **Idioma e Localização do Usuário Padrão**, a data, a hora e a formatação de números são automaticamente atualizadas para refletir sua escolha.

- No campo **Fuso Horário Padrão**, abra a lista e selecione o fuso horário preferido.

- No campo **Tempo Limite Padrão da Sessão do Usuário**, abra a lista e selecione o valor desejado.

h) Na área **Configurações de status e suspensão do usuário**, selecione as opções apropriadas a partir do seguinte:

- **Status do Usuário** permite que você **Suspenda** ou **Ative** usuários imediatamente; por exemplo, quando um usuário é bloqueado devido à digitação de senha incorreta por três vezes. Suas escolhas incluem:
  - **Ativo**
  - **Suspenso**
  - **Temporariamente suspenso até** abre um diálogo onde você insere a data apropriada para o fim da suspensão.
- **Auto-suspenção por login falhado** permite que você mitigue tentativas propositadas de comprometer senhas, tal como a força bruta. Suas escolhas incluem:
  - **Nunca auto-suspender usuário por falhas de login**
  - **Auto-suspender usuário após 3 tentativas de login falhadas**
  - **Auto-suspender temporariamente o usuário por 24 horas após 3 tentativas de login falhadas**

    Marque a caixa de seleção para **Enviar e-mail para todos os administradores se um usuário for suspenso devido a falha de login** porque esta ação pode representar uma ameaça de segurança e você pode querer examinar quaisquer alertas associados.
- **Auto-suspensão por inatividade** permite que você indique a suspensão apropriada para dispositivos que estão inativos. Suas escolhas incluem:
  - **Nunca auto-suspender por inatividade**
  - **Auto-suspender se o usuário não fizer login durante 30 dias**

i) Se a área **Remoção de Agentes** estiver disponível e você desejar permitir que este usuário faça solicitações de remoção de agentes, marque a caixa de seleção. Para mais informações, consulte "Gerenciando solicitações de remoção de agentes" na página 132.

Se você é o administrador de segurança, o diálogo Digite Código de Autorização é exibido, solicitando que você forneça autorização. Dependendo de que método de autenticação de segurança sua empresa escolheu, faça uma das seguintes ações:

- Para empresas que usam Tokens RSA SecurID para serviços de segurança:
  - Digite sua **Senha** da Central do Cliente.
  - Digite o **Código do Token SecurID** que aparece em seu Token RSA SecurID.

  Para mais informações, consulte "Usando Tokens RSA SecurID para Serviços de Segurança" na página 263.
- Para empresas que usam códigos de autorização enviados por e-mail para serviços de segurança:
  - Clique em **Gerar um novo token de autorização enviado por e-mail**. A página se atualiza e fornece confirmação de que uma mensagem de e-mail foi enviada para o endereço registrado para o administrador de segurança que está fazendo a solicitação.
  - Digite sua **Senha da Central do Cliente**.

- ○ Digite o **Código de Autorização** de Segurança que você recebeu na mensagem de e-mail.

  Para mais informações, consulte "Usando Códigos de Autorização Enviados por E-mail para Serviços de Segurança" na página 264.

5. Clique no botão **Salvar Alterações** para salvar as alterações, fechar a página Gerenciar Detalhes do Usuário, e atualizar a página Visualizar e Gerenciar Usuários com suas alterações.

Suspendendo um Usuário

IMPORTANTE Se você estiver suspendendo um administrador de segurança ou usuário de segurança avançado, siga as instruções na tarefa, "Removendo Acesso de Segurança para um Administrador de Segurança Específico" na página 261.

Para suspender um usuário:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.
2. No painel de navegação, clique em **Administração** > **Usuários** > link para **Ver e Gerenciar Usuários**.
3. Na página Ver e Gerenciar Usuários, adjacente ao usuário **Ativo** apropriado, clique no link **Editar**.

   NOTA Se você estiver conectado como um usuário avançado, pode suspender apenas os usuários Convidados.

4. Na página Gerenciar Detalhes do Usuário, na área **Configurações de status e suspensão do usuário**, nas opções **Status de Usuário**, escolha uma das seguintes opções:
   - Clique **Suspenso** para suspender este usuário indefinidamente.
   - Clique em **Temporariamente suspenso até** e no campo insira a data ou abra o calendário para selecionar a data quando a suspensão tiver terminado.
5. Clique em **Salvar Alterações** para suspender este usuário.

   Na página Ver e Gerenciar Usuários, a grelha de resultados se atualiza e mostra que este usuário está agora **Suspenso**.

   NOTA Se o usuário suspendo for um administrador de segurança ou um usuário de segurança avançado, todas as operações de segurança pendentes enviadas por este usuário serão processadas com habitualmente.

Ativando um usuário suspenso

Para ativar um usuário suspenso:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.
2. No painel de navegação, clique em **Administração** > **Usuários** > link para **Ver e Gerenciar Usuários**.

3. Na página Ver e Gerenciar Usuários, adjacente ao usuário **Suspenso** apropriado, clique no link **Editar**.

   NOTA Se você estiver conectado como um usuário avançado, pode habilitar apenas os usuários Convidados suspensos.

4. Na página Gerenciar Detalhes do Usuário, na área **Configurações de status e suspensão do usuário**, na área **Status do usuário**, clique **Ativo**.
5. Clique em **Salvar Alterações**.

   Na página Ver e Gerenciar Usuários, a grelha de resultados se atualiza e mostra que este usuário está agora **Ativo**.

Excluindo Usuários

Para excluir um usuário:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.
2. No painel de navegação, clique em **Administração** > **Usuários** > link para **Ver e Gerenciar Usuários**.
3. Na página Visualizar e Gerenciar Usuários, clique no link **Editar** do usuário que você deseja excluir.

   NOTA Se você estiver conectado como um usuário avançado, pode excluir apenas os usuários Convidados.

4. Quando a página Gerenciar Detalhes do Usuário abrir, clique em **Excluir**.

   Uma mensagem avisa você que está prestes a excluir a conta do usuário permanentemente.

5. Clique em **OK** para excluir este usuário. A página Visualizar e Gerenciar Usuários se atualiza e você verá uma linha de confirmação mostrando que o usuário foi excluído. A grelha de resultadosjá não mostra o usuário.

   NOTA Se o usuário excluído for um administrador de segurança ou um usuário de segurança avançado, todas as operações de segurança pendentes enviadas por este usuário serão processadas com habitualmente.

Conta

A seção de Contas da Central do Cliente inclui as seguintes seções:

- **Configurações de Conta:** Esta seção é onde você define e altera sua localização e fuso horário padrão, edita a atribuição automática de dispositivos sob a Garantia de Serviço e ligar ou desligar a coleção de dados de criptografia de discos completos para seus dispositivo.
- **Adicionar Licenças**: Esta seção permite que você adicione Licenças de agentes Computrace adicionais à sua conta.
- **Baixar Pacotes**: Esta seção fornece um link de download para todas as versões disponíveis do agente Computrace e dos pacotes do Absolute Manage preparados para sua conta.

- **Notificações do Sistema**: Esta seção permite que você indique que endereços de e-mail recebem mensagens de notificação do sistema quando as seguintes situações ocorrerem:
    - Dispositivos com a Garantia de Serviço Sem Chamadas
    - Licenças em Excesso / Expiradas
- **Desative Pré-autorizações**: Esta seção permite a Administradores de Segurança revogar todas os acordos de autorização no caso de uma violação de segurança.

    IMPORTANTE **Aja com cautela**. Desativando a Autorização de Segurança cancela todas as solicitações de operações de segurança existentes e suspende todos os Administradores de Segurança e Usuários de Segurança Avançados. Para ativar a autorização de segurança novamente, você deve contatar o Suporte Global Absolute. Para mais informações, consulte "Desativando Acesso de Segurança para todos os Usuários de Segurança Autorizados" na página 260.

- **Criar e Visualizar Solicitações de Remoção de Agentes**: Esta seção permite que funções de usuário com as autorizações apropriadas removam o Agente de um ou mais dispositivos.

Esta seção descreve as seguintes tarefas:

- Gerenciando Configurações de Conta
- Adicionando Licenças à sua Conta
- Baixando Pacotes para sua Conta
- Gerenciando Notificações do Sistema
- Gerenciando solicitações de remoção de agentes

Gerenciando Configurações de Conta

Esta seção oferece informações acerca dos seguintes tópicos:

- Editando Configurações de Conta
- Gerenciando Chamadas de Eventos para Sua Conta
- Gerenciando Licenças da Garantia de Serviço

Editando Configurações de Conta

Para editar suas configurações de conta:

1. Entre na Central do Cliente como um Administrador.

    NOTA Usuários avançados e convidados podem ver configurações de conta existente, mas não podem editá-las.

2. No painel de navegação, clique em **Administração** > **Conta** > **Configurações de Conta**.
3. Para alterar o idioma e formatos de exibição de hora padrão que aparecem em todas as páginas na Central do Cliente, selecione um valor da lista de **Idioma e Localidade Padrão**.
4. Para exibir a hora local em todas as páginas da Central do Cliente, selecione um valor da lista **Fuso Horário Padrão**.

5. Para desligar a auto-atribuição de licenças a dispositivos, desmarque a caixa de seleção **Atribuir automaticamente Licenças da Garantia de Serviço disponíveis a dispositivos**. Para informações sobre Licenças da Garantia de Serviço e como estas afetam sua conta, consulte "Gerenciando Licenças da Garantia de Serviço" na página 125.

6. Na área **Status da Criptografia de Disco Completo**, faça uma das seguintes ações:

   - Para ligar a coleção de dados da criptografia de discos completos dos dispositivos em sua conta, marque a caixa de seleção **Recolher dados de criptografia de discos completos dos dispositivos**.

     NOTA A coleção de dados de criptografia de discos completos é suportada somente para dispositivos Windows e Mac. Quando a recolha de dados for ligada, o processo de recolha inicia quando o dispositivo fizer a sua próxima chamada de agente. Portanto, dependendo da frequência de chamadas do agente, o Relatório do Status da Criptografia de Discos Completos pode ser atualizado dentro de um intervalo de tempo que varia desde poucos minutos até 24 horas.

   - Para parar a coleção de dados sobre a criptografia de discos completos dos seus dispositivos, desmarque a caixa de seleção **Coletar dados de criptografia de discos completos dos dispositivos**. Esta ação não irá eliminar quaisquer dados atuais ou históricos; no entanto, os alertas são suspensos automaticamente.
   - Se você desejar ligar a recolha de dados de criptografia de discos completos novamente, ative esta configuração e ative manualmente os alertas de criptografia. Para mais informações, consulte "Reativando Alertas Suspensos" na página 49.

   Para mais informações sobre a criptografia de discos completos, consulte "Relatório do Status de Criptografia de Discos Completos" na página 197.

7. Na área **Absolute Secure Drive**, faça uma das seguintes ações:

   - Para ligar a coleção de dados, marque a caixa de seleção **Coletar dados de logins falhados do Absolute Secure Drive dos dispositivos**. Para mais informações, consulte "Relatório de falhas de autenticação do Absolute Secure Drive" na página 195.

     NOTA Por padrão, a coleção de dados para logins falhados do Absolute Secure Drive está ligada para todas as contas.

   - Para desligar a coleção de dados,desmarque a caixa de seleção **Coletar dados de logins falhados do Absolute Secure Drive dos dispositivos**. Os dados recolhidos antes de desligar esta opção não são excluídos e continuam a aparecer no Relatório de falhas de autenticação do Absolute Secure Drive. Para mais informações, consulte "Relatório de falhas de autenticação do Absolute Secure Drive" na página 195.

8. Se você deseja que seus dispositivos do Windows gerenciados registrem a data e hora quando um arquivo foi acessado pela última vez, na área **Carimbo de data/hora do último acesso**, marque a caixa de seleção **Ativar carimbos de data/hora de último acesso de arquivo (apenas dispositivos do Windows**.

Se você usa a Exclusão de Dados, ative esta configuração para assegurar que quando seleciona a opção **Incluir Atributos de data do Arquivo** durante uma solicitação de Exclusão de Dados, a última data e hora estejam incluídas no arquivo de registro de Exclusões. Esta informação ajuda a determinar se uma violação de dados ocorreu em um dispositivo do Windows. Para mais informações sobre como solicitar uma operação de Exclusão de Dados, consulte "Iniciando uma solicitação de Exclusão de Dados" na página 271.

NOTA Em dispositivos executando um sistema operacional Windows Vista ou superior, a seguinte chave de registro controla o registro de carimbos de data/hora de acesso a arquivos:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate`
Por padrão , esta chave de registro está definida como "1". Quando você ativa a configuração **Carimbo de data/hora do último acesso**, a chave de registro é definida como "0" (zero), o que pode diminuir o desempenho ligeiramente em alguns dispositivos do Windows.

9. Para utilizar o posicionamento Wi-Fi do Google Maps™ para localizar seus dispositivos gerenciados, na área **Posicionamento Google Maps™**, marque a caixa de seleção **Usar a Geolocalização Google para pontos Wi-Fi**.

   Quando você ativa esta configuração:

   - O posicionamento Wi-Fi do Google Map pode ser usado para localizar seus dispositivos gerenciados. Para mais informações, consulte "Compreendendo Tecnologias de Localização" na página 219.
   - A opção do Posicionamento Wi-Fi do Google Maps™ está disponível e selecionada por padrão, nos relatórios do recurso de Cercas Geográficas e do Rastreamento de Geolocalização. Para mais informações, consulte os seguintes tópicos:
     - "Criando Cercas Geográficas" na página 299
     - "Relatórios de Rastreamento de Geolocalização" na página 217
   - A configuração está ocultada na página Configurações de Conta.

NOTA Esta configuração é aplicável apenas se o Rastreamento de Geolocalização estiver autorizado para a sua conta. Para mais informações, consulte "Autorizando Rastreamento por Geolocalização" na página 296.

10. Na área das **Configurações de RTT-IP**, faça quaisquer alterações às configurações de RTT-IP de toda a sua conta. Para mais informações sobre a RTT-IP e suas várias configurações consulte "Usando a Tecnologia de Tempo Real sobre IP" na página 249.
11. Na área **Configurações de chamadas**, configure se uma chamada de agente deverá ser realizada quando eventos específicos ocorrem nos dispositivos gerenciados da conta. Para mais informações, consulte "Gerenciando Chamadas de Eventos para Sua Conta" na página 119.

NOTA Chamadas de Eventos podem também ser gerenciadas a nível de dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.

12. Se a área **Chromebooks - Conta Google** estiver disponível, e você quiser gerenciar seus dispositivos Chrome na Central do Cliente, consulte "Gerenciando Dispositivos Chrome na Central do Cliente" na página 362.
13. Clique em **Salvar Alterações**.

Gerenciando Chamadas de Eventos para Sua Conta

Este recurso pode não estar disponível na sua conta, dependendo do produto da Central do Cliente que sua empresa adquiriu. Para mais informações sobre vários produtos, consulte "Níveis de Serviço" na página 20.

É possível ligar as chamadas de eventos para todos os dispositivos do Windows e Mac dentro de uma conta. As chamadas de eventos permitem que estes dispositivos gerenciados façam chamadas de agente quando um evento de alteração significativa ocorre em um dispositivo. Uma alteração a qualquer um dos atributos seguintes do dispositivo pode acionar uma chamada de eventos:

- localização de dispositivo
- configuração de hardware
- software instalado
- informação de rede (IP Público)
- usuário conectado

Para mais informações sobre os eventos de alteração que acionam uma chamada de eventos, .consulte "Eventos que Podem Acionar uma Chamada de Evento" na página 120.

Chamadas de eventos suplementam as chamadas agendadas que ocorrem automaticamente a partir de cada dispositivo gerenciado a cada 24,5 horas. No entanto, quando ocorre um chamada de evento, ela redefine o agendamento de chamadas regular. Tipicamente, quando as chamadas de eventos estão ligadas, as informações de dispositivos na Central do Cliente estão mais atualizadas, o que significa que os alertas são acionados em uma base mais atempada e seus relatórios são mais precisos.

Por exemplo, um dispositivo do Windows faz uma chamada de agente agendada para o Centro de Monitoramento às 9:00. Às 10:30 o IP público do dispositivo se altera, o que é considerado uma violação de regra, com base nas configurações feitas pelo administrador da Central do Cliente.

Um dos seguintes resultados pode ocorrer, dependendo de se as chamadas de eventos estão ligadas:

Chamadas de eventos ligadas?	Resultado
Sim	Um evento de alerta é acionada imediatamente, o que atualiza o endereço IP público do dispositivo na Central do Cliente. Se um alerta relacionado com um IP Público foi criado, a chamada de eventos aciona um alerta para notificar o administrador da Central do Cliente que uma violação de regra ocorreu. Se a RTT-IP estiver ativada na conta, o administrador da Central do Cliente solicita imediatamente uma operação de segurança, tal como um congelamento de dispositivo. Se o dispositivo estiver online, o agente é instruído no próximo ping de RTT-IP para fazer uma chamadas de agente completa e a operação de segurança é executada. Se o dispositivo estiver offline, a operação de segurança será executada na próxima reinicialização.

Chamadas de eventos ligadas?	Resultado
Não	A próxima chamada de agente agendada ocorrerá às 9:30 do dia seguinte (23 horas após o evento de alteração do IP público). O endereço IP público do dispositivo é atualizado na Central do Cliente. Se um alerta relacionado com um IP Público foi criado, a chamada de agente aciona um alerta para notificar o administrador da Central do Cliente que uma violação de regra ocorreu, mas até esse ponto, o dispositivo já terá estado fora da rede há 23 horas. Se a RTT-IP estiver ativada na conta, o administrador da Central do Cliente solicita imediatamente uma operação de segurança, tal como um congelamento de dispositivo. Se o dispositivo estiver online, a operação de segurança é realizada no próximo ping de RTT-IP, mas a RTT-IP por si só não acelera a iniciação do próprio alerta.
Para mais informações sobre alertas, consulte "Alertas" na página 38. Para mais informações sobre a RTT-IP, consulte "Usando a Tecnologia de Tempo Real sobre IP" na página 249.	

Esta seção oferece informações acerca dos seguintes tópicos:

- Eventos que Podem Acionar uma Chamada de Evento
- Noções Básicas Sobre o Período Mínimo das Chamadas de Eventos
- Ligando Chamadas de Eventos para Sua Conta
- Editando as Configurações de Chamadas de Eventos
- Desligando Chamadas de Eventos
- Visualizando a Lista de Dispositivos com as Chamadas de Eventos Ligadas

NOTA Por padrão, as chamadas de eventos estão desligadas para todos os dispositivos. É possível ligar as chamadas de eventos para todos os dispositivos do Windows ou Mac dentro de uma conta ou para dispositivos individuais gerenciados. Para mais informações sobre como ligar as Chamadas de Eventos para um dispositivo individual, .consulte "Editando Informações de Ativos" na página 141.

Eventos que Podem Acionar uma Chamada de Evento

Uma chamada de eventos é acionada quando um evento de alteração (alteração de um atributo no dispositivo) ocorre no dispositivo. A seguinte tabela descreve os eventos de alteração que podem ser configurados para acionar uma chamada de evento.

Descrição de eventos de alteração que acionam uma chamada de evento

Evento de alteração/ Opção de configuração	Descrição
Alteração de localização	Uma alteração na localização de um dispositivo Os hotspots Wi-Fi são usados para identificar alterações na localização do dispositivo. Se a intensidade do sinal ou a disponibilidade dos hotspots Wi-Fi armazenados em um dispositivo alterar, se considera que o dispositivo alterou sua localização. Um evento de alteração de localização é registrado apenas se o hotspot Wi-Fi atual indica que o dispositivo se deslocou 200 metros, que é o alcance médio de um hotspot Wi-Fi.

Descrição de eventos de alteração que acionam uma chamada de evento (continuado)

Evento de alteração/ Opção de configuração	Descrição
Alterações de Hardware	Uma alteração à memória, ao CPU ou ao disco rígido em um dispositivo Adicionando ou removendo os seguintes dispositivos não aciona uma alteração de hardware: ● Impressoras ● Dispositivos Firewire ● Dispositivos Thunderbolt ● Dispositivos Bluetooth **NOTA** Para se detectar uma alteração de hardware, o dispositivo necessita ser reiniciado. O inventário de hardware do dispositivo é comparado antes e depois da reinicialização. Se os inventários não corresponderem, um evento de alteração de hardware é registrado e uma chamada de evento é acionada.
Alterações de software	Uma alteração ao inventário de aplicativos de software instalados ou alterações ao sistema operacional do dispositivo
Alteração a usuário conectado	Uma alteração do usuário do dispositivo O nome de usuário do usuário atualmente conectado é comparado com o nome de usuário associado à sessão anterior. Se eles não corresponderem, um evento de alteração de usuário é registrado e uma chamada de evento é acionada. Em dispositivos com Windows, um evento de alteração de usuário é registrado quando o recurso Trocar Usuário é usado.
Alterações de rede	Uma alteração ao endereço IP público de um dispositivo Quando o endereço IP local de um dispositivo gerenciado se altera, o endereço IP público do dispositivo é verificado para determinar se também mudou. Se sim, um evento de alteração de rede é registrado e uma chamada de evento é acionada.

Noções Básicas Sobre o Período Mínimo das Chamadas de Eventos

Quando você configura as chamadas de eventos, você precisa especificar o período mínimo da chamada de eventos, que controla o período de tempo mínimo que deve passar entre as chamadas realizadas a partir de um dispositivo. Esta configuração permite que você determine com que frequência um dispositivo realiza chamadas para o Centro de Monitoramento quando múltiplos eventos de alteração ocorrem em um dispositivo em sucessão rápida.

O objetivo da configuração do Período mínimo das Chamadas de Eventos é reduzir o fluxo de trafego desnecessário para os gateways de sua rede. É recomendado que experimente as várias configurações para determinar a configuração ótima para sua empresa.

Os valores possíveis são:

- 15 minutos
- 20 minutos
- 30 minutos
- 45 minutos
- 2 horas
- 3 horas
- 4 horas
- 6 horas

- 1 hora

Exemplo
Chamadas de eventos são ativadas em um dispositivo e o Período mínimo das Chamadas de Eventos é definido para **2 Horas**. No dia seguinte, duas alterações de software ocorrem no dispositivo, com um intervalo de 10 minutos. A primeira alteração de software aciona uma chamada de evento imediatamente, ma a segunda chamada deve esperar para o período de chamada de evento mínimo a expirar. Uma alteração de rede ocorre então no dispositivo 20 minutos após a segunda alteração de hardware. Nenhuma chamada de eventos é realizada porque o Período mínimo das Chamadas de Eventos ainda não expirou. O Período mínimo das Chamadas de Eventos expira duas horas depois da primeira chamada de eventos. Uma nova chamada de evento é acionada a partir do dispositivo para enviar os detalhes da segunda alteração de software e da alteração de rede ao Centro de Monitoramento.

Ligando Chamadas de Eventos para Sua Conta

Por padrão, as chamadas de eventos estão desligadas a nível de conta. Para ligar as chamadas de eventos para todos os dispositivos em sua conta:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Configurações de Conta**.
3. Na página Configurações de Conta, role para a área **Configurações de Chamada**.
4. Clique no campo e selecione uma das seguintes opções:
   - **Definir as configurações de chamada para todos os dispositivos habilitados**: Ligar as chamadas de eventos para todos os dispositivos do Windows e Mac existentes e recém-ativados. Assim que novos dispositivos do Windows e Mac forem ativados, ligue as Chamadas de Eventos e aplique as configurações de chamada especificadas.
   - **Definir as configurações de chamada para dispositivos novos**: Assim que novos dispositivos do Windows e Mac forem ativados, ligue as Chamadas de Eventos e aplique as configurações de chamada especificadas.
   - **Ligar as chamadas de eventos para todos os dispositivos em que as chamadas de eventos estejam desligadas**: Ligar as chamadas de eventos somente para dispositivos do Windows e Mac existentes:
5. Na lista **Período Mínimo das Chamadas de Evento** selecione a quantidade mínima de tempo que deve passar entre chamadas de agente a partir de um dispositivo. Os valores possíveis variam entre 15 minutos e 6 horas. Para mais informações, consulte "Noções Básicas Sobre o Período Mínimo das Chamadas de Eventos" na página 121.
6. Todas as **Opções de configuração** estão selecionadas por padrão. Para excluir uma ou mais **Opções de configuração**, limpe cada caixa de seleção aplicável.

   NOTA Para mais informações sobre cada opção, focalize sobre ⓘ adjacente às **Opções de Configuração**. Para informações detalhadas sobre as alterações de dispositivo associadas a cada opção,consulte "Eventos que Podem Acionar uma Chamada de Evento" na página 120.

7. Clique em **Salvar Alterações**. As chamadas de eventos são ativadas em cada dispositivo na próxima chamada de agente agendada.

   NOTA Se você selecionou uma opção de configuração de chamada que se aplica a dispositivos recém-ativados, o **Período Mínimo das Chamada de Eventos** e as **Opções de Configuração** que serão aplicados nesses dispositivos aparecem sob **Configurações de chamada padrão atuais para novos dispositivos**.

Editando as Configurações de Chamadas de Eventos

Se as Chamadas de Eventos estiverem ligadas a nível de conta, você pode editar o **Período Mínimo de Chamadas de Eventos** e as **Opções de Configuração** a qualquer momento.

Para editar as configurações de chamadas para dispositivos associados à conta:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Configurações de Conta**.
3. Na página Configurações de Conta, role para a área **Configurações de Chamada**.
4. Clique no campo e selecione uma das seguintes opções:
   - **Definir as configurações de chamada para todos os dispositivos habilitados**: Atualize as configurações de chamada para dispositivos Windows e Mac existentes e recém-ativados.
   - **Definir as configurações de chamada para dispositivos novos**: Atualize as configurações de chamada somente para dispositivos Windows e Mac recententemente ativados.
   - **Alterar as configurações de chamada para todos os dispositivos em que as chamadas de eventos estejam ligadas**: Atualize as configurações de chamada para dispositivos Windows e Mac existentes que têm as chamadas de eventos ligadas. Se as chamadas de eventos foram desligadas para um ou mais dispositivos a nível de dispositivos, aqueles dispositivos permanecem inalterados.
   - **Ligar as chamadas de eventos para todos os dispositivos em que as chamadas de eventos estejam desligadas**: Ligar as chamadas de eventos para os seguintes dispositivos do Windows e Mac:
     - Dispositivos com Chamadas de Eventos desligadas a nível de dispositivos
     - Dispositivos recém-ativados sem as chamadas de eventos ligadas

     NOTA Esta opção está disponível apenas se as Chamadas de Eventos estiverem ligadas a nível de conta, mas estará desligada para alguns dispositivos. Para mais informações sobre como gerenciar chamadas de eventos a nível de dispositivo, .consulte "Configurando as Chamadas de Eventos para um Dispositivo" na página 146.
5. Edite o **Período mínimo das Chamadas de Eventos**. Os valores possíveis variam entre 15 minutos e 6 horas. Para mais informações, consulte "Noções Básicas Sobre o Período Mínimo das Chamadas de Eventos" na página 121.
6. Edite as **Opções de configuração** ao selecionar ou limpar cada caixa de seleção aplicável.

NOTA Para mais informações sobre cada opção, focalize sobre ⓘ adjacente às **Opções de Configuração**. Para informações detalhadas sobre as alterações de dispositivo associadas a cada opção,consulte "Eventos que Podem Acionar uma Chamada de Evento" na página 120.

7. Clique em **Salvar Alterações**. As configurações de chamada atualizadas são ativadas em cada dispositivo na próxima chamada de agente agendada.

Desligando Chamadas de Eventos

Se as Chamadas de Eventos estiverem ligadas a nível de conta, você pode desligá-las para todos os dispositivos na conta.

NOTA Para desligar as chamadas de eventos para dispositivos individuais, consulte "Configurando as Chamadas de Eventos para um Dispositivo" na página 146.

Para desligar as chamadas de eventos para todos os dispositivos na conta:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Configurações de Conta**.
3. Na página Configurações de Conta, role para a área **Configurações de Chamada**.
4. Clique no campo e selecione **Desligar as chamadas de eventos**.
5. Clique em **Salvar Alterações**. As chamadas de eventos são desligadas em cada dispositivo na próxima chamada de agente agendada.

Visualizando a Lista de Dispositivos com as Chamadas de Eventos Ligadas

Para visualizar a lista de dispositivos gerenciados que têm as chamadas de eventos ligadas:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Configurações de Conta**.
3. Na página Configurações de Conta, role para a área **Configurações de Chamada**.
4. Sob **Dispositivos com chamadas de eventos ligadas** , clique em **Visualizar**. Um diálogo se abre.
5. Filtre a lista de dispositivos usando qualquer dos seguintes critérios:
   - **Identificador**: um número de série eletrônico único atribuído ao agente instalado em um dispositivo
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo
   - **Nome de Dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
   - **Número de Série**: o número de série do dispositivo ou outro hardware.
   - **Configurações de Chamadas de Eventos**: as opções de configuração ativas quando as chamadas de eventos foram ligadas
   - **Período mínimo das Chamadas de Eventos**: o período de tempo selecionado quando as Chamadas de Eventos foram ligadas

- **Motivo da Última Chamada**: o motivo da última chamada de agente do dispositivo. Os valores possíveis são **Agendado** ou **Evento | <tipo de alteração>**.

NOTA Os resultados não podem ser filtrados pela **Hora da Última Chamada** que é a data e a hora da última chamada de agente a partir do dispositivo.

6. Ordene a lista ao clicar em um cabeçalho de coluna.

NOTA Não é possível ordenar as colunas de **Configurações de Chamadas de Eventos** ou **Motivo da Última Chamada**.

7. Para visualizar a página do Resumo do Dispositivo para um dispositivo, clique no link de **Identificador**.
8. Clique em **Cancelar** para fechar o diálogo.

Gerenciando Licenças da Garantia de Serviço

Quando um dispositivo que está atribuído a uma licença da Garantia de Serviço é furtado e a Absolute Software não consegue recuperar o dispositivo ou executar uma operação de Exclusão de Dados, você poderá estar elegível para receber um pagamento da Garantia de Serviço para esse dispositivo. Para estarem elegíveis para receber esse pagamento, na altura de um furto, os dispositivos em sua conta têm de estar corretamente sinalizados como estando elegíveis para a Garantia de Serviço.

Um dos seguintes cenários é possível:

- **Sua conta inclui produtos Computrace com a Garantia de Serviço e você tem licenças disponíveis**: Por norma, se sua conta na Central do Cleinte incluir produtos Computrace com a Garantia de Serviço, e você ainda tiver licenças disponíveis, uma licença da Garantia de Serviço é automaticamente atribuída a cada dispositivo novo e estes dispositivos ficam elegíveis para receberem pagamentos da Garantia do Serviço.

  IMPORTANTE Se você desativar a função de atribuição automática de licenças da Garantia de Serviço, você terá que manualmente atribuir a licença de Garantia de Serviços a dispositivos aplicáveis em sua conta. Para mais informações sobre a atribuição manual da Garantia de Serviço, consulte "Editando Manualmente a Atribuição de Licenças da Garantia de Serviço" na página 126.

- **Sua conta inclui produtos Computrace com a Garantia de Serviço mas você não tem licenças disponíveis**: Se sua conta contiver mais dispositivos do que licenças, a atribuição automática de licenças a dispositivos é desativada até você adicionar mais licenças à sua conta ou você remover manualmente a licença da Garantia de Serviço de alguns dispositivos.

  Por exemplo, se você tiver 1000 licenças do Computrace Complete, e 1250 dispositivos a contatar o nosso Centro de Monitoramento, então 250 dispositivos não foram atribuídos licenças, nem estão elegíveis para a garantia de serviço.

  Para informações sobre como adicionar licenças à sua conta, consulte "Adicionando Licenças à sua Conta" na página 126. Para mais informações sobre como remover manualmente licenças da Garantia de Serviço de dispositivos, consulte "Editando Manualmente a Atribuição de Licenças da Garantia de Serviço" na página 126.

- **Sua conta contém produtos tanto com como sem a Garantia de Serviço**: Se sua conta contiver uma mistura de produtos Computrace, em que alguns produtos incluem a Garantia de Serviço e outros não, as licenças da Garantia de Serviço para a sua conta podem estar incorretamente atribuídas.

  Para atender a um problema desse gênero, você deverá editar a atribuição de licenças da Garantia de Serviço manualmente. Para mais informações, consulte "Editando Manualmente a Atribuição de Licenças da Garantia de Serviço" na página 126.

Editando Manualmente a Atribuição de Licenças da Garantia de Serviço

É possível atribuir ou remover a Licença da Garantia de Serviço para cada dispositivo individualmente ou usar os grupos de dispositivos para fazer a alteração.

- **Editando o valor para um único dispositivo**: Se você quiser atribuir ou remover a licença da Garantia de Serviço para um único dispositivo, você pode usar a página Visualizar ou Editar Campos Definidos pelo Usuário para o dispositivo.
  - Para atribuir a licença da Garantia de Serviço a um dispositivo, abra a página Visualizar ou Editar Campos Definidos pelo Usuário, abra a lista **Tem Garantia de Serviço**, e clique **Sim**.
  - Para remover a Licença da Garantia de Serviço de um dispositivo, abra a página Visualizar ou Editar Campos Definidos pelo Usuário, abra a lista de **Tem Garantia de Serviço**, e clique em **Não**.

  Para mais informações, consulte "Atribuindo Valores de Dados a Um Dispositivo Individual" na página 60.
- **Editando o valor para um grupo de dispositivos**: A maneira mais rápida para se atribuir ou remover manualmente uma licença da Garantia de Serviço de dispositivos existe em criar um grupo de dispositivos e alterar o valor de **Tem Garantia de Serviço**.

  Para alterar a atribuição de licenças da Garantia de Serviço para um grupo de dispositivos:

  a) Crie um grupo de dispositivos contendo os dispositivos para os quais você deseja atribuir ou remover licenças da Garantia de Serviço. Por exemplo, se você quiser atribuir a Garantia de Serviço a todos os funcionários que trabalham no departamento de Vendas, crie um grupo de dispositivos que contém os dispositivos de todos os funcionários nesse departamento.

  b) Abra a página Visualizar e Editar Campos Definidos pelo Usuário para o grupo de dispositivos que você acabou de criar na etapa a, abra a lista **Tem Garantia de Serviço**, e clique em **Sim** para atribuir ou **Não** para remover as licenças da Garantia de Serviço, conforme o que se aplica. Para informações sobre como alterar um campo definido pelo usuário para um grupo de dispositivos, consulte "Atribuindo Valores de Dados a Todos os Dispositivos em um Grupo de Dispositivos" na página 60.

Adicionando Licenças à sua Conta

A página Adicionar Licenças permite que você adicione Licenças de agentes adicionais à sua conta. As licenças de um determinado produto são agrupadas e vendidas como Chaves de Produto. Por exemplo, 10 licenças do Computrace Complete com um contrato de 3 anos podem ser agrupadas como uma única Chave de Produto.

As Chaves de Produto são disponibilizadas pelo seu revendedor ou podem ser compradas diretamente da Absolute Software.

NOTA Para mais informações sobre a compra de licenças adicionais, entre em contato direto com a Absolute Software em: www.absolute.com/en/about/contact/corporate.

Para adicionar licenças à sua conta:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Adicionar Licenças**.
3. Na página Adicionar Licenças, digite o grupo de chave de seu produto e depois clique em **Adicionar**. Repita este processo para adicionar todas as chaves adicionais.
4. Depois de digitar todas as Chaves de Produto, clique em **Salvar**. Você recebe uma mensagem de confirmação indicando que sua conta está sendo configurada. Novos arquivos do agente são criados para suas licenças adicionais.
5. Depois de registrar todas as suas Chaves de Produto, siga para a página **Baixar Pacotes** e faça download do seu agente. O widget de **Resumos de Licenças** na home page também é atualizada e mostra as licenças adicionais para sua conta. Para mais informações, consulte "O Painel de controle e Seus Widgets" na página 30.

Baixando Pacotes para sua Conta

Dependendo do produto da Central do Cliente que sua empresa adquiriu, a página Baixar Pacotes pode conter as seguintes seções:

- A seção **Agentes para os Sistemas Operacionais Windows, Mac e Móveis** permite que você baixe todos os pacotes de instalação do agente para sua conta. Para mais informações, consulte "Baixando o Agente Computrace" na página 127.

  NOTA Pacotes de instalação do agente não estão disponíveis para dispositivos iPad e dispositivos Chrome. Para mais informações sobre como gerenciar dispositivos iPad e iPad mini, consulte "Computrace Mobile Theft Management para dispositivos iPad" na página 345. Para mais informações sobre como gerenciar Chromebooks e Chromeboxes, consulte "Computrace Mobile Theft Management Mobile Theft Management para Dispositivos Chrome" na página 361. Para receber mais informações sobre suporte para o agente Computrace em sistemas operacionais baseados em Linux, tais como Ubuntu 14.04 LTS ou Debian® 7.x, contate o Suporte Global. Consulte "Contatando o Suporte Global da Absolute Software" na página 23.

- A seção do **Absolute Manage** permite que você baixe os pacotes de instalação do Absolute Manage para sua conta. Para mais informações, consulte "Usando o Absolute Manage Suite" na página 128.

Baixando o Agente Computrace

A seção Agentes na página Baixar Pacotes fornece links para todos os pacotes de instalação do agente que tenham sido *carimbados* para sua conta. As seguintes informações estão listadas para cada pacote de instalação:

- **Tipo de Agente**: tipo de agente específico por plataforma. O agente é atualmente compatível com as plataformas do Windows, Mac, Windows Mobile, Android e BlackBerry.
- **Versão do Agente**: O número da versão (compilação) do agente.
- **Última Atualização**: a data e a hora da criação dos arquivos do agente.

- **Último Download**: a data e a hora em que os arquivos de agente foram baixados a última vez da Central do Cliente.

Para mais informações sobre o agente Computrace, consulte "Compreendendo a Função do Agente Computrace" na página 20.

Para baixar os arquivos de instalação do agente carimbados:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Baixar Pacotes**.

   A página Baixar Pacotes se abre com uma lista de todos os **Tipos de Agentes** e as **Versões de Agentes** que são criadas para sua conta.

   NOTA Para ver a versão atual do agente Computrace, abra a dica de ferramenta **Versões atualizadas de Agentes disponíveis**. Entre em contato com o Suporte Global da Absolute para atualizar para a versão mais atual do agente, se necessário.

3. Na seção **Agente para Windows, Mac e Sistemas Operacionais Móveis**, clique no link apropriado na coluna **Tipo de Agente**.
4. Siga as instruções da tela para concluir o download.

   Depois de instalar o agente em um dispositivo cliente, o dispositivo é automaticamente associado à sua conta.

É também possível abrir a página Baixar Pacotes a partir da Home Page, clicando no link **Baixar Pacotes** na parte inferior da página, abaixo do **Painel de controle**.

Para mais informações sobre como instalar o agente em plataformas diferentes, consulte o *Guia do Administrador do Agente Computrace* disponível na página Documentação na Central do Cliente.

Atualizando para a Última Versão do Agente

Periodicamente, a Absolute Software lança uma nova versão do Agente. Quando um novo agente for disponibilizado, um anúncio será colocado na home page. Se você estiver executando uma versão mais antiga do agente e quiser atualizá-lo, contate o Suporte Global da Absolute Software em www.absolute.com/support. Um representante do suporte cria novos arquivos do agente para você e informa-lhe quando os arquivos estão prontos para download na página Baixar Pacotes.

IMPORTANTE A lista de agentes na página Baixar Pacotes não é atualizada automaticamente quando uma nova versão do agente é lançada. É necessário entrar em contato com o Suporte Global da Absolute, se você desejar atualizar o seu agente.

Usando o Absolute Manage Suite

A suite Absolute Manage é uma solução multi-plataforma única, sem emendas, de gerenciamento de clientes para gerenciar todas suas estações de trabalho Mac OS e Windows em uma única consola unificada na plataforma de sua escolha. Todos os componentes do Absolute Manage, incluindo o servidor, consola de administração e os clientes podem ser misturados e combinados a partir de qualquer plataforma. Os administradores de rede e de sistemas muitas vezes descobrem que existem várias maneiras de realizar a mesma tarefa no Absolute Manage, e cabe a eles decidir qual delas se encaixa no fluxo de trabalho da empresa e funciona melhor no ambiente de computação proprietário.

Os pacotes de instalação do Absolute Manage disponíveis na seção Absolute Manage permitem que administradores extraiam, baixem e usem os dados coletados pelos agentes em dispositivos gerenciados. Para as contas que incluem o Absolute Manage, os dados que estavam anteriormente disponíveis apenas através de relatórios na Central do Cliente, agora estão disponíveis usando o aplicativo do Absolute Manage no dispositivo local.

A seção de Absolute Manage permite que você execute as seguintes funções:

- Baixando os pacotes de instalação do Absolute Manage
- Carregando um Agente Carimbado Incluindo o Absolute Manage

Baixando os pacotes de instalação do Absolute Manage

Para baixar os pacotes de Absolute Manage para seu sistema operacional:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Baixar Pacotes**.
3. Na página Baixar Pacotes, na seção do Absolute Manage, clique no link apropriado a partir do seguinte:
   - **Baixar Absolute Manage para Computadores Windows**
   - **Baixar Absolute Manage para Computadores Macintosh**
4. Siga as instruções da tela para concluir o download.
5. Instale o aplicativo Absolute Manage em seu dispositivo. Quando solicitado, forneça o **Código de Registro** e o **Número de Série** disponíveis na página Baixar Pacotes.

   NOTA O **Código de Registro** e o **Número de Série** exibidos na seção do Absolute Manage são específicos para sua conta.

Carregando um Agente Carimbado Incluindo o Absolute Manage

Dispositivos gerenciados usando o servidor do Absolute Manage contêm um agente especial. É possível criar uma versão modificada do Pacote de Instalação do agente para reinstalar o agente, contendo componentes do Absolute Manage, caso o agente em um de seus dispositivos gerenciados seja removido. A área de Persistência do Absolute Manage na seção do Absolute Manage na página Baixar Pacotes permite que você carregue versões modificadas dos Pacotes de Instalação do Agente para Windows e para Mac para uso em uma data posterior.

NOTA Dependendo das licenças de que você é proprietário, a seção do Absolute Manage pode não estar disponível, mas a área de Persistência do Absolute Manage pode aparecer em sua própria seção.

Para garantir que o arquivo seja carregado com êxito, o pacote de instalação do agente deve estar de acordo com os seguintes requisitos:

- O pacote deve ser um arquivo .zip válido Quaisquer erros de extração de pacotes levam a um erro de falha de validação e à falha no processo de carregamento.
- O pacote de instalação pode ter qualquer nome, contanto que ele seja um arquivo de .zip válido. O nome de arquivo muda para um nome gerado pelo sistema no momento de um carregamento bem-sucedido.

- O pacote precisa conter as pastas e arquivos mostrados na seguinte tabela , dependendo do sistema operacional.

Detalhes dos pacotes de instalação para os sistemas operacionais Windows e Mac

Sistema Operacional de Dispositivo	Detalhes do Pacote de Instalação
Windows	O pacote deve conter os seguintes arquivos: ● `\Absolute Manage Agent\0x0409.ini` ● `\Absolute Manage Agent\AgentVersion.exe` ● `\Absolute Manage Agent\Data1.cab` ● `\Absolute Manage Agent\DefaultDefaults.plist` ● `\Absolute Manage Agent\Info.plist` ● `\Absolute Manage Agent\instmsiw.exe` ● `\Absolute Manage Agent\LANrev Agent.msi` ● `\Absolute Manage Agent\LANrevAgentSafeInstaller.exe` ● `\Absolute Manage Agent\LANrevAgentUpdater.bat` ● `\Absolute Manage Agent\LANrevAgentUpdater.exe` ● `\Absolute Manage Agent\LANrevAgentUpdater_Launcher.bat` ● `\Absolute Manage Agent\setup.exe` ● `\Absolute Manage Agent\Setup.ini` **NOTA** O arquivo DefaultDefaults.plist deve conter uma configuração **ServerList** com pelo menos um servidor de inventário preliminar e um endereço. Para mais informações, conecte-se ao AMRC, abra o *Guia de Introdução do Absolute Manage* e consulte as informações sob o título “Implantando o agente usando o instalador local”. O arquivo Info.plist deve conter um elemento XML **CFBundleGetInfoString** com o conteúdo apropriado e válido.
Mac	O pacote deve conter os seguintes arquivos e pastas: ● `\Absolute Manage Agent\Certificates` **NOTA** A pasta Certificados deve conter três arquivos `.pem`. ● `\Absolute Manage Agent\Absolute Manage Agent.pkg` ● `\Absolute Manage Agent\DefaultDefaults.plist` ● `\Absolute Manage Agent\DetermineDeploymentPlatform.sh` ● `\Absolute Manage Agent\InstallAgent.sh` ● `\Absolute Manage Agent\SpecialSSLUpdater.plist`

Para carregar um pacote de instalação do agente modificado:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Baixar Pacotes**.
3. Na página Baixar Pacotes, role para o local do Absolute Manage.
4. Na área de **Persistência do Absolute Manage**, clique **Navegar** na área para o sistema operacional aplicável (**Windows** ou **Mac**).

5. No diálogo Carregar Arquivos, navegue para o local no disco rígido local de seu dispositivo para localizar o apropriado arquivo .zip de instalação do agente.
6. Clique no nome de arquivo e em seguida clique em **Abrir** para selecionar o arquivo. A página Baixar Pacotes é atualizada para listar o nome do arquivo no campo **Nome do arquivo** na seção da **Persistência do Absolute Manage**.
7. Clique em **Carregar**. O arquivo é carregado para a Central do Cliente e a página Baixar Pacotes se atualiza e exibe o arquivo na tabela **Nome do Arquivo** para o sistema operacional aplicável.

Gerenciando Notificações do Sistema

A página Notificações do Sistema permite que os administradores da Central do Cliente configurem uma lista de destinatários para as mensagens de notificação do sistema. As notificações do sistema são mensagens geradas automaticamente para avisar aos usuários de problemas potenciais com as contas.

Por exemplo, se um de seus dispositivos coberto com a Garantia de Serviço parar de chamar o Centro de Monitoramento, a notificação de sistema **Dispositivos com a Garantia de Serviço Sem Chamada** avisa que o dispositivo não está chamando mais.

As notificações do sistema são enviadas por e-mail para a lista de destinatários. Provavelmente você deseja incluir todos os administradores de sistema da Central do Cliente em sua lista de destinatários. Há um limite de 20 destinatários por notificação.

Esta seção descreve as seguintes tarefas:

- Atualizando a página Notificações do Sistema
- Dispositivos com a Garantia de Serviço Sem Chamadas
- Resolvendo uma Disparidade do Sinalizador de Recuperação

Atualizando a página Notificações do Sistema

Para atualizar a página Notificações do Sistema:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Notificações do Sistema**.
3. Na página Notificações do Sistema, clique no separador apropriado e edite a lista de endereços de e-mail.
4. Clique em **Salvar**.

Dispositivos com a Garantia de Serviço Sem Chamadas

A notificação do sistema **Dispositivos com Garantia de Serviço Sem Chamada** avisa os destinatários que um ou mais dispositivos cobertos pela Garantia de Serviço pararam de chamar para o Centro de Monitoramento.

Para editar a notificação do sistema Dispositivos com a Garantia de Serviço Sem Chamadas:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Notificações do Sistema**.
3. Na página Notificações do Sistema, clique no separador **Dispositivos com a Garantia de Serviço Sem Chamadas** e faça uma das seguintes ações:

- Para adicionar destinatários, selecione a opção **Ativar Notificações para Todos os Endereços de E-mail Abaixo** e digite os endereços de e-mail dos destinatários desejados no campo **Endereços de E-mail para Notificação**.

  NOTA É possível adicionar um máximo de vinte (20) endereços de e-mail neste campo. Separe cada entrada com um ponto-e-vírgula.

- Para remover destinatários, selecione a opção **Desativar Notificações para Todos os Endereços de E-mail Abaixo** e digite os endereços de e-mail dos destinatários desejados no campo **Endereços de E-mail para Notificação**. Para remover simultaneamente vários destinatários, separe cada entrada com um ponto-e-vírgula. Clique em **Salvar** para salvar as alterações.
- Para desativar a notificação do sistema, selecione a opção **Desativar Notificações para Todos os Endereços de E-mail Abaixo** e remova todos os endereços de e-mail da lista de destinatários.

4. Clique em **Salvar**.

Resolvendo uma Disparidade do Sinalizador de Recuperação

A notificação do sistema **Disparidade do Sinalizador de Recuperação** avisa os destinatários que o número de dispositivos com o sinalizador de recuperação excede o número de licenças compradas com o serviço de recuperação.

Para resolver uma disparidade de sinalizador de recuperação:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Notificações do Sistema**.
3. Na página Notificações do Sistema, clique no separador **Disparidade do Sinalizador de Recuperação** e faça uma das seguintes ações:
   - Para adicionar recipientes, digite os endereços de e-mail dos destinatários desejados no campo **Endereços de E-mail para Notificação**.

     NOTA É possível adicionar um máximo de vinte (20) endereços de e-mail neste campo. Separe cada entrada com um ponto-e-vírgula.

   - Para remover destinatários, remova os endereços de e-mail dos destinatários desejados no campo **Endereços de E-mail para Notificação**. Certifique-se de que todas as entradas remanescentes estejam separadas por um ponto-e-vírgula, sem espaços.
   - Para desativar a notificação do sistema, remova todos os endereços de e-mail da lista de destinatários.
4. Clique em **Salvar**.

Gerenciando solicitações de remoção de agentes

Em contas na Central do Cliente com vários dispositivos, pode haver alguns dispositivos que já não são mais funcionais ou que estão sendo retirados de serviço devido a um ou vários motivos. Os administradores de TI precisam remover o agente de tais dispositivos e liberar as licenças em uso.

A Central do Cliente permite que você remova o agente de um ou mais dos seus dispositivos, que estes dispositivos façam ou não parte de um grupo de dispositivos. Dependendo de como sua conta na Central do Cliente está configurada, Administradores de Segurança, Usuários Administradores ou designados Usuários Avançados podem usar o recurso de auto-atendimento de remoção de agentes para criar novas solicitações de remoção do agente, bem como gerenciar as solicitações existentes.

Os dois cenários seguintes podem ocorrer:

- Se sua conta na Central do Cliente contém pelo menos um Administrador de Segurança, os seguintes usuários podem usar o recurso de auto-atendimento de remoção de agentes.
  - Todos os Administradores de Segurança
  - Administradores que são designados por Administradores de Segurança
- Se sua conta na Central do Cliente não contém nenhum Administrador de Segurança, os seguintes usuários podem usar o recurso de auto-atendimento de remoção de agentes.
  - Todos os Administradores
  - Usuários avançados que são designados por Administradores

NOTA Para mais informações sobre como conceder autorização para a remoção de agentes, consulte "Criar Novos Usuários" na página 108.

Esta seção fornece informações sobre os seguintes tópicos e tarefas:

- Requisitos Mínimos do Sistema para Remoção de Agentes
- Criando uma solicitação de remoção de agentes nova

NOTA Para informações sobre como desativar um dispositivo Chrome usando uma solicitação de remoção de agentes, consulte "Desativando Dispositivos Chrome " na página 374.

Requisitos Mínimos do Sistema para Remoção de Agentes

Atualmente, a função de auto-atendimento de remoção de agentes está disponível para dispositivos que atendem aos seguintes requisitos mínimos do sistema:

- O dispositivo está ligado e executando um sistema operacional suportado. Consulte "Plataformas Suportadas para o Agente Computrace" na página 22.

  IMPORTANTE Se você quiser remover o agente de um dispositivo executando qualquer outro sistema operacional, entre em contato com o Suporte Global da Absolute Software. Para mais informações, consulte "Contatando o Suporte Global da Absolute Software" na página 23.

- O dispositivo não possui nenhuma solicitação ativa de remoção de agentes ou uma das operações de segurança ativa.

  Você não pode remover o agente de um dispositivo nas seguintes condições:
  - O dispositivo não está ligado e executando um dos sistemas operacionais obrigatórios. **Consulte "Plataformas Suportadas para o Agente Computrace" na página 22.**
  - O dispositivo possui uma solicitação de removação de agentes em andamento.
  - O dispositivo foi relatado como furtado e tem um relatório de furto aberto. Você dever cancelar o Relatório de Furto antes de continuar. Para obter informações sobre como relatar o furto de um dispositivo, consulte "Relatando o Furto de um Dispositivo Gerenciado" na página 377.

- O dispositivo está atribuído a uma política de Congelamento de Dispositivo do Estado Offline. Se o dispositivo furtado estiver atribuído a uma política de Congelamento de Dispositivo do Estado Offline, você deve remover o dispositivo da política do Estado Offline antes de continuar. Para mais informações, consulte "Removendo Dispositivos de uma Política do Estado Offline" na página 320.
  - O dispositivo foi congelado por uma solicitação de Congelamento de Dispositivo ou uma política de Congelamento de Dispositivo do Estado Offline. Se o dispositivo furtado estiver congelado, você deve descongelar o dispositivo antes de continuar. Para mais informações, consulte "Descongelando um Dispositivo Congelado" na página 327.
  - Possui um Absolute Secure Drive e/ou usa um produto de criptografia de discos completos, mas não passou a autorização de pré-inicialização do vendedor necessária para ambas as formas de criptografia de discos completos.
  - O dispositivo possui uma solicitação de recuperação de arquivos remota ativa. Você deve cancelar a solicitação de Recuperação de Arquivos antes de continuar. Para obter mais informações sobre como cancelar uma solicitação de recuperação de arquivos, consulte "Cancelando uma Solicitação de Recuperação de Arquivo" na página 337.

Criando uma solicitação de remoção de agentes nova

É possível usar um dos seguintes métodos para selecionar os dispositivos de destino para criar uma nova solicitação de remoção de agentes.

- Usando a Caixa de Diálogo da Central do Cliente
- Usando um Arquivo de Texto

IMPORTANTE Antes de criar uma nova solicitação de remoção de agentes, confirme que nenhuma solicitação de remoção de agentes ou operações de segurança estão pendentes no dispositivo. Para mais informações, consulte "Requisitos Mínimos do Sistema para Remoção de Agentes" na página 133.

Usando a Caixa de Diálogo da Central do Cliente

Este método permite que você selecione os dispositivos de destino interativamente, usando o diálogo na Central do Cliente.

Para remover o agente de um dispositivo elegível:

1. Conecte-se à Central do Cliente como um usuário a quem foi concedido autorização para criar solicitações de remoção de agentes. Para mais informações, consulte os seguintes tópicos:
   - "Gerenciando solicitações de remoção de agentes" na página 132
   - "Criar Novos Usuários" na página 108
2. Se sua empresa usa códigos de autorização enviados por e-mail para serviços de segurança, solicite um código de autorização ao completar a tarefa, "Solicitando um Código de Autorização de Segurança" na página 265.
3. No painel de navegação, clique em **Administração** > **Conta** > **Criar e Visualizar Solicitações de Remoção de Agentes**.
4. Na página Criar e Visualizar Solicitações de Remoção de Agentes, clique em **Criar nova solicitação para Remoção de Agentes**.
5. No diálogo de Selecionar Dispositivo(s) para Remoção de Agentes, faça o seguinte:

a) No campo **onde o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado para mostrar uma lista de dispositivos de qual você precisa remover os agentes.

b) Se você deseja mostrar dispositivos que cumprem critérios específicos, digite as informações apropriadas nos campos adjacente a **e o campo**.

   Por exemplo, você pode querer exibir apenas os dispositivos onde o campo **Nome de Usuário começa com** a palavra **Absolute**.

c) Por padrão, a lista de dispositivos exibida na grelha de resultados é limitada a apenas aqueles dispositivos a partir dos quais você pode remover o agente. Se você deseja exibir todos os dispositivos que correspondem aos critérios que você especificou, limpe a caixa de seleção **Mostrar apenas dispositivos elegíveis**.

d) Por padrão, todos os dispositivos que correspondem a seus critérios especificados são mostrados na lista. Se você quer mostrar apenas os dispositivos que estão dormentes, selecione a caixa de seleção **Mostrar Apenas Dispositivos Dormentes**.

e) Clique em **Filtrar**. A caixa de diálogo Selecionar Dispositivo(s) para Remoção de Agentes é atualizada e mostra uma lista de dispositivos que satisfazem os seus critérios.

f) Na grelha de resultados, selecione os dispositivos ao fazer uma das seguintes ações na coluna da extrema esquerda, que exibe caixas de seleção:

   - Para selecionar dispositivos individuais, marque as caixas de seleção para aqueles dispositivos só.
   - Para selecionar todos os dispositivos mostrados apenas nesta página, marque a caixa de seleção no cabeçalho.
   - Para selecionar todos os dispositivos que atenderam aos critérios de filtragem, focalize seu mouse sobre a seta na caixa de seleção do cabeçalho. Clique no link **Selecionar todos os registros (<n>)** para selecioná-los todos. A caixa de diálogo Selecionar Dispositivo(s) para Remoção de Agentes é aberta com os dispositivos especificados que você selecionou.

6. Clique em **Continuar** para abrir o diálogo de Definir Dispositivo(s) para Autorização de Remoção de Agentes.

7. Se você é um administrador de segurança, você será solicitado a fornecer autorização. Dependendo de que método de autenticação de segurança sua empresa escolheu, faça uma das seguintes ações:

   - Para empresas que usam Tokens RSA SecurID para serviços de segurança:
     i) Digite sua **Senha da Central do Cliente**.
     ii) Digite o **Código do Token SecurID** que aparece em seu Token RSA SecurID.
   - Para empresas que usam códigos de autorização enviados por e-mail para serviços de segurança:
     i) Digite sua **Senha da Central do Cliente**.
     ii) Digite o **Código de Autorização** de Segurança que você recebeu na mensagem de e-mail.

8. Clique em **Definido para remoção**. Uma solicitação de remoção de agentes para os dispositivos que você selecionou é criada e executada na próxima chamada do agente.

Usando um Arquivo de Texto

Se você já conhece os identificadores ou números de série dos dispositivos dos quais você deseja excluir o agente, você pode carregar um arquivo de texto para a Central do Cliente para criar uma solicitação de remoção de agentes.

É possível inserir uma lista de dispositivos em uma única coluna, separando cada entrada com uma linha nova (pressione `Enter`). Não utilize pontuação nesta lista.

Para carregar um arquivo de texto de dispositivos nos quais você deseja solicitar uma remoção de agentes:

1. Conecte-se à Central do Cliente como um usuário a quem foi concedido autorização para criar solicitações de remoção de agentes. Para mais informações, consulte os seguintes tópicos:
   - "Gerenciando solicitações de remoção de agentes" na página 132
   - "Criar Novos Usuários" na página 108
2. No painel de navegação, clique em **Administração** > **Conta** > **Criar e Visualizar Solicitações de Remoção de Agentes**.
3. Na página Criar e Visualizar Solicitações de Remoção de Agentes, clique em **Carregar lista de dispositivos para Remoção de Agente**.
4. No diálogo Carregar lista de dispositivos para Remoção de Agente, em **Caminho do Arquivo**, digite o caminho completo para o arquivo de texto ou clique em **Navegar** para selecioná-lo a partir de seu computador local.
5. Selecione uma das seguintes como o tipo de lista de arquivos:
   - **Identificadores**
   - **Números de Série**

   IMPORTANTE Números de série Lenovo com sete caracteres podem ser associados com mais de um dispositivo e pode causar erros quando você carrega uma lista de dispositivos usando um arquivo de texto. Quando você carrega uma lista de dispositivos Lenovo, use números de série completos ou Identificadores de dispositivo Computrace, ambos os quais são únicos para cada dispositivo gerenciado.
6. Faça uma das seguintes opções:
   - Se você for um Administrador de Segurança:
     i) Clique em **Carregar Arquivo**.
     Você é solicitado a fornecer autorização. Dependendo de que método de autenticação de segurança sua empresa escolheu, faça uma das seguintes ações:
       - Para empresas que usam Tokens RSA SecurID para serviços de segurança:
         – Digite sua **Senha da Central do Cliente**.
         – Digite o **Código do Token SecurID** que aparece em seu Token RSA SecurID.

         Para mais informações, consulte "Usando Tokens RSA SecurID para Serviços de Segurança" na página 263.
       - Para empresas que usam códigos de autorização enviados por e-mail para serviços de segurança:

- Clique em **Solicitar Código de Autorização**. A página se atualiza e fornece confirmação de que uma mensagem de e-mail foi enviada para o endereço registrado para o administrador de segurança que está fazendo a solicitação.
- Digite sua **Senha da Central do Cliente**.
- Digite o **Código de Autorização** de Segurança que você recebeu na mensagem de e-mail.

Para mais informações, consulte "Usando Códigos de Autorização Enviados por E-mail para Serviços de Segurança" na página 264.

ii) Clique em **Definir para Remoção**. Uma solicitação de remoção de agentes para os dispositivos que você selecionou é criada e executada nos dispositivos de destino na próxima chamada do agente. A página Criar e Visualizar Solicitações de Remoção de Agentes se abre.

- Se você for um Administrador, clique em **Carregar Arquivo e Definir para Remoção**. Uma solicitação de remoção de agentes para os dispositivos que você selecionou é criada e executada na próxima chamada do agente.

Você verá uma mensagem para confirmar o upload do arquivo. A mensagem também mostra o número total de entradas e o número total de entradas falhadas, caso existam, no arquivo de texto.

NOTA Para ver o arquivo de registro do último carregamento de arquivo, clique em **Ver arquivo de registro**. Alternativamente, você pode acessar o arquivo de registro na página **Meus Relatórios**.

Capítulo 4:   Gerando Relatórios

Este capítulo descreve como utilizar a Central do Cliente para gerar relatórios com base nos dados que o Computrace agente coleta de dispositivos monitorados. É possível personalizar e filtrar os relatórios para focalizar áreas de interesse chave. Para detalhes específicos sobre cada relatório da Central do Cliente, consulte "Trabalhando com Relatórios" na página 152.

Na Central do Cliente, você abre o relatório que deseja usando o painel de navegação, define os critérios de filtragem apropriados e gera os resultados de relatório. É possível também baixar o relatório de resultados nos formatos CSV ou XML. Para os seguintes relatórios, os resultados estão apenas disponíveis nos formatos CSV ou XML:

- Relatório de Impressora
- Relatório de Monitores
- Relatório do Resumo de Auditoria da Microsoft
- Relatório do Resumo do Uso da Licença
- Relatório Perfis de Chamadas
- Relatório de Auditoria do Usuário

Quando você cria um relatório personalizado, pode salvar os critérios de filtragem do relatório. É possível recuperar relatórios salvos em visitas subsequentes à Central do Cliente e gerar novamente o relatório para exibir resultados atualizados.

NOTA Quando um relatório é salvo, os critérios de filtragem são salvos em vez dos resultados porque os dados se alteram ao longo do tempo.

Várias tarefas são comuns à maioria de relatórios da Central do Cliente, incluindo:

- Executando Relatórios
- Navegando por Relatórios
- Editando Informações de Ativos
- Imprimindo Relatórios
- Salvando Filtros de Relatório
- Editando Filtros de Relatório Salvos
- Baixando Relatórios
- Segurança Multinível

Executando Relatórios

Para uma visão geral de cada relatório da Central do Cliente, consulte "Trabalhando com Relatórios" na página 152.

Para executar e exibir um relatório na Central do Cliente:

1. Conectar-se à Central do Cliente, que abrirá a home page da Central do Cliente.

NOTA Dependendo da função de usuário a que você está atribuído, só é possível ver aqueles relatórios que são designadas como apropriados para essa função de usuário. Para mais informações, consulte "Funções de usuário e seus direitos de acesso" na página 96.

2. No painel de navegação, clique no link **Relatórios**.
3. Abra o relatório que você deseja ao fazer uma das seguintes ações:
   - Na página **Relatórios**, clique no relatório que deseja executar.
   - No painel de navegação, clique na categoria que contém o relatório que você deseja executar e clique no link desse relatório.
4. Se necessário, clique em **Aceitar** para aceitar os termos e condições de execução do relatório.
5. No painel de **Critérios de Pesquisa**, especifique como os resultados do relatório devem ser filtrados.

NOTA Quando aberto pela primeira vez, alguns relatórios retornam resultados com base em critérios de filtro padrão. Para informações sobre como usar o recurso Escolher, consulte "Usando o Recurso Escolher" na página 140.

6. Clique em **Mostrar Resultados**. Se nenhum registro coincidir com seus critérios de filtro, a Central do Cliente mostra a mensagem **Nenhum registro coincide com seus critérios de pesquisa**.

NOTA Para obter informações sobre como baixar arquivos CSV ou saídas XML para os relatórios que a Central do Cliente exibe na tela, consulte "Baixando Relatórios" na página 150.Para informações sobre como elaborar relatórios com os resultados apenas disponíveis para download, consulte "Trabalhando com Relatórios" na página 152.

Se a sua sessão na Central do Cliente expirar enquanto você está visualizando um relatório, uma mensagem de aviso de esgotamento de tempo se abre com instruções sobre como continuar.

Navegando por Relatórios

Para navegar pelos relatórios, existem alguns recursos comuns, que são apontados a seguir:

- Expandindo e Recolhendo as Informações dos Critérios de Pesquisa
- Usando o Recurso Escolher
- Visualizando uma Linha Inteira em um Registro de Relatório
- Deslocando-se Entre as Páginas do Relatório
- Alterando o Número de Registros que Aparecem no Relatório
- Alterando a Ordem de Classificação

Expandindo e Recolhendo as Informações dos Critérios de Pesquisa

Os critérios de pesquisa podem ser expandidos ou recolhidos . Dependendo da seção de Critérios de Pesquisa estar expandida ou recolhida, respectivamente, estes botões exibem as setas para cima ou para baixo.

Usando o Recurso Escolher

Muitas áreas da Central do Cliente requerem que o usuário insira dados específicos, como um Identificador ou número de série. Para evitar o erro humano, a maioria dos relatórios inclui o botão de **Escolher**.

Para usar o recurso Escolher:

1. Clique em **Escolher** em qualquer página. O dialogo de Escolher se abre e exibe uma lista de todos os valores disponíveis e válidos para o campo de dados.
2. Clique no valor desejado para selecioná-lo.

   Um indicador de progresso se abre para dar informações sobre o processo de seleção. Quando o processamento estiver completo, o valor selecionado é inserido no campo apropriado do filtro do relatório.

Visualizando uma Linha Inteira em um Registro de Relatório

Colunas na grelha de resultados de um relatório são apresentadas em um formato horizontal, com colunas e linhas. Arraste a barra de rolagem na parte inferior da página para a direita para ver a linha inteira de um registro de relatório.

Deslocando-se Entre as Páginas do Relatório

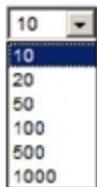
É possível passar para várias localizações em um relatório, da seguinte forma:

- à primeira página ao clicar em **<<Primeira** ou o link para a página número **1**
- à página anterior ao clicar em **<Ant**
- para uma página específica ao clicar no **link** para o número da página que você deseja
- à próxima página ao clicar **Próxima>**
- à última página ao clicar **Última>>**

Alterando o Número de Registros que Aparecem no Relatório

O número padrão de registros mostrados em cada relatório depende do relatório. Por exemplo, quando você abre um relatório, poderá ver 10 acima e abaixo da grelha de resultados no seu lado direito.

Para alterar o número de registros que aparecem em um relatório:

1. Entre na Central do Cliente e abra o relatório desejado. Consulte "Executando Relatórios" na página 138.
2. Altere o valor padrão ao abrir a lista.
3. Selecione o número apropriado de registros a exibir no relatório a partir destas opções:

Alterando a Ordem de Classificação

Inicialmente, a maioria de relatórios é ordenado pelo **Identificador**, no entanto, você pode ordenar usando qualquer cabeçalho de coluna.

Para ordenar um relatório por outros critérios:

1. Entre na Central do Cliente e abra o relatório desejado. Consulte "Executando Relatórios" na página 138.
2. Na grelha de resultados, clique no título de coluna por qual você deseja ordenar o relatório.

Editando Informações de Ativos

Cada dispositivo em que o Computrace agente está instalado é atribuído um identificador único pelo Centro de Monitoramento. Clique em um Identificador para abrir a página do Resumo do Dispositivo, onde você pode atualizar as informações associadas a um dispositivo em particular. Por exemplo, se um Identificador for transferido para um novo dispositivo, você pode alterar as informações do dispositivo conectado àquele Identificador.

NOTA Para detalhes sobre como ver a página Resumo do Dispositivo de um dispositivo Chrome, consulte "Visualizando Informações de Dispositivo de um Dispositivo Chrome" na página 365.

Para editar a informação associada a um dispositivo:

1. Entre na Central do Cliente e abra o relatório desejado, seguindo a tarefa "Executando Relatórios" na página 138.
2. Em qualquer relatório, clique no **Identificador** que você deseja editar, que abrirá a página Resumo do Dispositivo.

   A página Resumo do Dispositivo fornece informações sobre o dispositivo.

   Algumas informações nesta página são editáveis e outras são de somente leitura. Para mais informações sobre como trabalhar com as informações da página Resumo do Dispositivo, consulte "Informações de Dispositivo na Página Resumo do Dispositivo" na página 142.

   NOTA Dependendo do tipo de dispositivo, alguns valores do Resumo do Dispositivo não são preenchidos. Por exemplo, se o Identificador for um dispositivo com Windows Mobile, somente o subconjunto de informações de hardware e software relevantes para dispositivos com Windows Mobile são mostrados.

3. Se você alterou quaisquer informações de dispositivo, clique em **Salvar Alterações**. A página Resumo de Dispositivos é atualizada e confirma que suas alterações foram salvas.
4. Para gerar novamente o relatório e visualizar quaisquer modificações, clique no link **Voltar**.

   NOTA Para voltar ao relatório, clique no botão de **Voltar** do navegador. Note que retornar não atualiza o relatório com as alterações. Você deve gerar o relatório novamente para ver suas modificações.

Informações de Dispositivo na Página Resumo do Dispositivo

A página Resumo do Dispositivo fornece as seguintes informações sobre o dispositivo:

- **Identificador**, que é um identificador único para este dispositivo
- **Marca**
- **Modelo**
- **Número de Série**[1]
- **RTT-IP** somente para dispositivos do Windows
  Para mais informações sobre esta seçao, consulte "Ativando a RTT-IP para um Dispositivo Individual" na página 252.
- **Configurações de Chamada** somente para dispositivos Windows e Mac
  Para mais informações sobre esta seção, consulte "Editando Informações de Ativos" na página 141.
- **Nome de Dispositivo**
- **Nome completo do dispositivo Windows** somente para dispositivos do Windows
- **Domínio do Windows** somente para dispositivos do Windows
- **Nome de Dispositivo**
- **Nome completo do dispositivo Windows** somente para dispositivos do Windows
- **Domínio do Windows** somente para dispositivos do Windows
- **Grupo de Trabalho** somente para dispositivos do Windows
- **Departamento**, que você pode editar
- **Nome de Usuário Detectado**
- **Nome de Usuário Atribuído**, que você pode editar.
  Para mais informações, consulte "Usando o campo de Nome de Usuário Atribuído" na página 148.
- **Endereço de e-mail de usuário atribuído**, que você pode editar
- **Número de Ativo Detectado**
- **Número de ativo atribuído**, que você pode editar
- **Grupos de Dispositivos** mostra os grupos de dispositivos a quais este dispositivo gerenciado pertence.
  Para editar um grupo de dispositivos, clique no link do grupo de dispositivos desejado. Para mais informações, consulte "Editando um Grupo de Dispositivos" na página 82.

IMPORTANTE É possível editar valores nos campos **Departamento**, **Nome de Usuário Atribuído**, **Endereço de e-mail de usuário atribuído**, e **Número de Ativo Atribuído.** Se você editar quaisquer deste campos, clique em **Salvar Alterações.**

Mais informações sobre o dispositivo estão disponíveis nos seguintes separadores:

- Separador do Resumo do Hardware
- Separador do Resumo de Software
- Separador do Rastreamento de Chamadas

[1]Ao detectar números de série de discos rígidos, o agente Computrace consulta o controlador de disco em primeiro lugar. Se isso falhar, então o agente usa a Interface de Gerenciamento do Windows da Microsoft (WMI) para obter os números de série dos discos rígidos. Seja o que for que a WMI relatar, que é fornecido pela Microsoft ou pelo seu fornecedor de hardware e/ou de software, o mesmo aparece no Relatório de Configurações de Hardware e de Alterações do SO. Para uma descrição da Microsoft de um cenário onde este problema pode ocorrer, consulte: connect.microsoft.com/VisualStudio/feedback/details/623282/win32-physicalmedia-returns-incorrect-serial-number-on-vista-or-higher-when-run-as-standard-user

Separador do Resumo do Hardware

O separador do **Resumo de Hardware** fornece informações sobre os seguintes pontos de identificação:

NOTA Valores listados na seção do Resumo do Hardware para **Marca Detectada**, **Modelo Detectado** e **Número de Série Detectado** são capturados pelo agente e podem ser diferentes dos valores inseridos manualmente e listados na seção **Resumo de Ativos**.

- **Marca Detectada**
- **Modelo Detectado**
- Os valores dos números de **Série Detectados** mostrados na seção do Resumo de Ativos para a **Marca Detectada**, o **Modelo Detectado**, e o número de **Série Detectado** são capturados pelo Computrace agente e podem variar dos valores inseridos manualmente e fornecidos na seção Resumo do Ativo.
- **CPU**
- **RAM**
- **Informação do Disco Rígido** mostra as informações detectadas sobre os discos rígidos instalados no dispositivo, que inclui:
  - **Unidades Físicas**: o nome da partição do**Disco** rígido detectada e o **Número de Série** para cada
  - **Volume**: o nome da partição do disco rígido detectada
    - **Tipo**: o tipo de disco rígido
    - **Sistema de Arquivos**: o método de armazenamento e organização dos dados e arquivos salvos no dispositivo
    - **Espaço Total**: a soma da capacidade de armazenamento usada e inutilizada no disco rígido
    - **Espaço Livre**: a capacidade de armazenamento inutilizada do disco rígido
- **Adaptadores de Banda Larga Móvel**: se você estiver usando o recurso de Tecnologia de Tempo Real esta área fornece as seguintes informações sobre qualquer um destes modems detectados no dispositivos. Para mais informações sobre a RTT, consulte "Usando a Tecnologia de Tempo Real" na página 242.
  - **Fabricante**: o nome do fabricante do adaptador de banda larga móvel
  - **Modelo**: o número do modelo do adaptador de banda larga móvel
  - **Rede**: o fornecedor de serviço móvel associado ao adaptador de banda larga móvel
  - **Status do Serviço**: a disponibilidade da rede
  - Link de **Detalhes**: clique no link para acessar o diálogo dos detalhes do adaptador de banda larga móvel. Para mais informações sobre este diálogo, consulte "Visualizando Informações de Adaptadores de Banda Larga Móvel" na página 245.
  - **Número de Telefone Detectado**: o número de telefone associado ao adaptador de banda larga móvel, relatado pelo dispositivo
  - **Número de Telefone Substituto**: o número de telefone alternativo ou substituto associado ao adaptador de banda larga móvel

    NOTA Se o Computrace não detectar o número de telefone automaticamente, o dispositivo envia automaticamente um SMS para o Centro de Monitoramento. O endereço de "responder para" recebido com o SMS torna-se no valor para o campo de **Número de Telefone Substituto**. O valor do campo do **Número de Telefone de Substituição** tem precedência sobre o valor do campo do **Número de Telefone Detectado** quando você envia mensagens SMS para dispositivos gerenciados. Para mais informações, consulte "Editando o Número de Telefone Substituto" na página 246.

- **Tentar Chamada Forçada**: envia uma solicitação de uma chamada imediata do agente ao dispositivo, via SMS

NOTA Os relatórios de Adaptadores de Banda Larga Móvel e as Chamadas Iniciadas pelo Centro de Monitoramento (MCIC) estão atualmente disponíveis apenas para dispositivos que rodam o Windows. Estes recursos não estão disponíveis em dispositivos Macintosh.
Antes de usar a Tecnologia de Tempo Real (Real Time Technology - RTT), incluindo o rastreamento de ativos de adaptadores de banda larga móvel, as Chamadas Iniciadas pelo Centro de Monitoramento, e Solicitações de Bloqueio por SMS, você precisa ativar esses recursos para a sua conta ou para dispositivos gerenciados individuais dentro da sua conta. Entre em contato com seu representante da Absolute Software para ativar estas funções.

- **Rádios de Rede Móvel**: Esta área é exibida se quaisquer rádios são detectados em um dispositivo móvel. As seguintes informações estão disponíveis:
  - **Tipo de Rádio**: o rádio de rede móvel disponível no dispositivo. Os valores possíveis são:
    - **GSM** (Sistema Global para Comunicação Móvel)
    - **CDMA** (Acesso Múltiplo por Divisão de Código)
  - **ID do Equipamento**: o número de identificação único para o dispositivo móvel.
  - **ID do Assinante**: o número único associado ao assinante; armazenado no rádio de rede, o chip Módulo de Identificação do Assinante (SIM) ou equivalente.
  - **Número de Telefone Detectado**: o número de telefone associado ao dispositivo móvel, como relatado pelo dispositivo.
  - **Número de Telefone Substituto**: o número de telefone alternativo ou substituto associado ao dispositivo móvel. Se o Computrace não detectar o número de telefone automaticamente, o dispositivo envia automaticamente um SMS para o Centro de Monitoramento. O endereço de "responder para" do SMS se torna no valor para o campo **Número de Telefone Substituto**. Para mais informações, consulte "Editando o Número de Telefone Substituto" na página 246.
  - **Tentar chamada forçada**: use este recurso para forçar uma chamada de SMS a partir do agente do dispositivo para o Centro de Monitoramento.
- **Ver detalhes do hardware**: fornece mais informações sobre o hardware do dispositivo.

  Clique para abrir a lista para ver a seguinte informação detectada:
  - **IP Local**
  - **Descrição do Cartão de Rede 1**
  - **IP do Cartão de Rede 1**
  - **Endereço MAC do Cartão de Rede 2**
  - **Número de CPUs**
  - **Versão de BIOS do Sistema**
  - **Profundidade de Cor do Monitor de Vídeo**
  - **IP do Proxy**
  - **Endereço MAC do Cartão de Rede 1**
  - **Descrição do Cartão de Rede 2**
  - **IP do Cartão de Rede 2**
  - **Data do BIOS do Sistema**
  - **Descrição do Dispositivo de Vídeo**

- **Resolução do Monitor de Vídeo**

NOTA O relatório do Driver da Impressora fornece uma lista de todos os drivers de impressoras instalados no dispositivo. Para baixar este relatório, clique no link **Baixar Relatório da Impressora**. Este relatório é idêntico ao Relatório de Impressora, exceto que estes resultados são limitados aos drivers de impressoras instalados neste dispositivo.

Separador do Resumo de Software

O separador do Resumo de Software fornece informações sobre os seguintes pontos de identificação:

- **Relatório de Software por Dispositivo**: um link para este relatório onde você pode consultar todos os aplicativos de software detectados pelo agente em um dispositivo gerenciado. Para mais informações, consulte "Relatório de Software por Dispositivo" na página 174.
- **Sistema Operacional**
- **Service Pack do SO**
- **Anti-malware Detectado**
- **Chave de Produto do SO**
- **Ver Hotfixes da Microsoft instalados**: a tabela que mostra a seguinte informação sobre os pacotes instalados:
  - **Aplicativo**
  - **Nome do Pacote**
  - **Número do Hotfix**
  - **Detalhes**
  - **Instalado por** nome
  - **Instalado em** data

Separador do Rastreamento de Chamadas

O separador Rastreamento de Chamadas fornece informações sobre a operação do agente, incluindo:

- **Relatório do Histórico de Chamadas**: um link a este relatório. Para ver detalhes sobre **Informações Estendidas de Chamadas de IP**, clique no link sob a coluna **Endereço de IP Público** na grelha de resultados do relatório.
- **O agente foi instalado pela primeira vez em (primeira chamada)**: data e hora da primeira chamada de agente ao Centro de Monitoramento
- **Versão do agente**: versão e número do agente
- **Agente realizou a última chamada em**: data e hora da última chamada de agente ao Centro de Monitoramento
- **Última chamada do agente feita de**: Endereço IP a partir de onde o agente realizou a última chamada
- **Próxima Chamada do agente esperada em**: data e hora da próxima chamada de agente ao Centro de Monitoramento
- **Dados de rastreamento do ativo coletados pela última vez em**: a data e a hora que os dados do rastreamento foram colectados pela última vez

- Se o dispositivo estiver equipado com a funcionalidade de Rastreamento por Geolocalização, o separador Rastreamento de Chamadas também exibe a **Última localização conhecida** e a **Data de determinação da localização** para o dispositivo.

  NOTA Para visualizar o Relatório de Histórico de Chamadas deste Identificador, vá para o Relatório de Histórico de Chamadas. Para obter informações detalhadas sobre o rastreamento de IPs ou de ID do chamador, clique no endereço de IP ou no número telefônico listados no campo **o agente fez a sua última chamada a partir de**. A página Informações de Chamadas Estendidas se abre. Esta página lista os detalhes sobre a localização do endereço IP ou do número de telefone. Consulte "Executando Relatórios" na página 138.

- O separador de **Registro de Chamadas Forçadas**, que fornece informações sobre todas a tentativas de chamadas forçadas no dispositivo usando mensagens SMS. Consulte "Visualizando o Registro de Chamadas Forçadas" na página 246.

  NOTA Este separador aparece apenas se a Tecnologia de Tempo Real (RTT) e as Chamadas Iniciadas pelo Centro de Monitoramento (MCIC) estão ativas no dispositivo. Consulte "Usando a Tecnologia de Tempo Real" na página 242.

Gerenciando Chamadas de Eventos para um Dispositivo

Este recurso pode não estar disponível na sua conta, dependendo do produto da Central do Cliente que sua empresa adquiriu. Para mais informações sobre vários produtos, consulte "Níveis de Serviço" na página 20.

É possível usar a área Configurações de Chamada da página do Resumo do Dispositivo para configurar Chamadas de Eventos para o dispositivo. As chamadas de eventos são independentes de e vêm por acréscimo às chamadas de agente agendadas normais que ocorrem automaticamente a partir de cada dispositivo gerenciado.

IMPORTANTE As chamadas de eventos podem ser ligadas a nível de conta ou de dispositivo. Para mais informações sobre as Chamadas de Eventos, e instruções para as ligar a nível de conta, consulte "Gerenciando Chamadas de Eventos para Sua Conta" na página 119.

Configurando as Chamadas de Eventos para um Dispositivo

Para configurar Chamadas de Eventos para um dispositivo gerenciado:

1. Navegue até à área **Configurações de Chamada** da página Resumo do Dispositivo.
2. Faça uma das seguintes opções:
   - Para ligar as chamadas de eventos:
     i) Selecione a caixa de seleção **Ligar as chamadas de eventos para o dispositivo**.

     NOTA As chamadas de eventos são ativadas quando o dispositivo fizer sua próxima chamada de agente agendada. O campo **Chamada Programada** mostra a frequência atual de chamadas programadas do dispositivo.

     ii) Na lista **Período Mínimo das Chamadas de Evento** selecione a quantidade mínima de tempo que deve passar entre chamadas de agente a partir de um dispositivo. Os valores possíveis variam entre 15 minutos e 6 horas.

Para mais informações, consulte "Noções Básicas Sobre o Período Mínimo das Chamadas de Eventos" na página 121.

iii) Todas as **Opções de configuração** estão selecionadas por padrão. Para excluir uma ou mais **Opções de configuração**, limpe cada caixa de seleção aplicável.

NOTA Para mais informações sobre cada opção, focalize sobre ⓘ adjacente às **Opções de Configuração.** Para informações detalhadas sobre as alterações de dispositivo associadas a cada opção, consulte "Eventos que Podem Acionar uma Chamada de Evento" na página 120.

- Para editar as configurações de chamadas existentes para um dispositivo que tem as chamadas de eventos ligadas:

  i) Edite o **Período mínimo das Chamadas de Eventos**. Os valores possíveis variam entre 15 minutos e 6 horas. Para mais informações, consulte "Noções Básicas Sobre o Período Mínimo das Chamadas de Eventos" na página 121.

  ii) Edite as **Opções de configuração** ao selecionar ou limpar cada caixa de seleção aplicável.

NOTA Para mais informações sobre cada opção, focalize sobre ⓘ adjacente às **Opções de Configuração**. Para informações detalhadas sobre as alterações de dispositivo associadas a cada opção,consulte "Eventos que Podem Acionar uma Chamada de Evento" na página 120.

- Para desligar as Chamadas de Eventos, limpe a caixa de seleção **Ligar as chamadas de eventos para o dispositivo**.

3. Clique em **Salvar Alterações**.

   As chamadas de eventos são configuradas em cada dispositivo na próxima chamada de agente agendada.

Visualizando o Histórico de Chamadas de um Dispositivo

É possível ver detalhes sobre as chamadas de agente realizadas a partir de um dispositivo Windows ou Mac nos últimos 365 dias.

Para ver o histórico de chamadas de um dispositivo:

1. Navegue até à área **Configurações de Chamada** da página Resumo do Dispositivo.

   O campo **Motivo da Última Chamada** mostra os detalhes da chamada de agente mais recente a partir do dispositivo. Os valores possíveis são:

   - **Agendado**
   - **Evento | <tipo de alteração>**

   Por exemplo: **Evento | Software removido, Software instalado, Usuário conectado alterado**

2. Clique **Ver Histórico de Chamadas** para abrir o diálogo do Histórico de Chamadas.

   As seguintes informações sobre cada chamada de agente são fornecidas:

   - **Hora da Chamada**: a data e a hora da chamada
   - **Motivo**: o tipo de chamada de agente

Para chamadas de eventos, o tipo de alteração é fornecida. Os valores possíveis são:

- **Localização alterada**
- **Hardware alterado**
- **Software instalado**
- **Software removido**
- **Usuário conectado alterado**
- **IP público alterado**

Para mais informações sobre estas alterações, consulte "Eventos que Podem Acionar uma Chamada de Evento" na página 120.

3. Para ordenar a informação, clique no título de coluna desejado.
4. Para fechar o diálogo, clique em **Cancelar**.

Usando o campo de Nome de Usuário Atribuído

O campo de **Nome do Usuário Atribuído** na página do Resumo do Dispositivo é um campo estático e editável que permite que os Administradores identifiquem a quem um dispositivo foi originalmente atribuído. O campo estático é útil em empresas onde os IDs de rede de usuários finais não são fáceis de identificar.

Também, em muitas empresas, os membros das equipes trocam seus dispositivos periodicamente. Nestes ambientes, um ID de rede ou endereço de e-mail não identifica com precisão o proprietário real de um dispositivo.

Para mais informações sobre como definir o campo **Nome de Usuário Atribuído**, consulte "Editando Informações de Ativos" na página 141.

NOTA O campo de **Nome de Usuário Atribuído** é anexado a todos os downloads de relatórios que incluem um **Identificador** ou **Nome de Usuário**, independentemente do campo de**Nome de Usuário Atribuído** ser incluído no próprio relatório da Central do Cliente.

Usando o campo de Dispositivos Dormentes

O campo **Dormente** ajuda os administradores a distinguir aqueles dispositivos que estão verdadeiramente desaparecidos daqueles que estão localizados em sítios sem acesso à internet, tais como instalações de armazenamento.

O campo **Dormente** é um campo estático e editável que os administradores podem usar para identificar dispositivos que não são esperados manter contato com o Centro de Monitoramento. Para mais informações sobre como definir campos definidos pelo usuário, consulte "Visualizando e Editando Campos de Dados" na página 59.

Definindo dispositivos como **Dormente** exclui-os do relatório de Dispositivos Desaparecidos e dos widgets de Taxa de Chamadas de agentes. Para mais informações, consulte os seguintes tópicos:

- "Relatório de Dispositivos em Falta" na página 210
- "O Painel de controle e Seus Widgets" na página 30

Imprimindo Relatórios

É possível imprimir os relatórios por inteiro ou em partes. Cada página de um relatório inclui um ícone de **Imprimir**, tal como .

NOTA Por padrão, a página atual mostra 10 registros do relatório completo. Para imprimir uma maior seleção de registros, abra a lista de **Por Página** e selecione o número desejado de registros para exibir na página.

Para gerar uma versão da página atual de um relatório para impressão, que está otimizada para a criação de uma cópia impressa:

1. Entre na Central do Cliente e abra o relatório desejado. Consulte "Executando Relatórios" na página 138.
2. Abra qualquer página de relatório e clique em .
3. A página atual é baixada para uma planilha do Microsoft Excel e você pode imprimir a página do relatório usando o Excel.

Salvando Filtros de Relatório

A maioria dos relatórios permite a você editar os dados exibidos. É possível salvar relatórios personalizados usando o recurso **Salvar Filtro de Relatório**.

NOTA Relatórios salvos definem critérios para um relatório e não os dados existentes. Os dados reais, que atendem aos critérios, mudam de acordo com o momento, alterando assim os conteúdos do relatório salvo.

Para salvar um filtro de relatório:

1. Entre na Central do Cliente e abra o relatório desejado. Consulte "Executando Relatórios" na página 138.
2. Em qualquer página de relatório, clique .
3. No diálogo de Salvar Filtro de Relatório, digite um nome (até 48 caracteres) para o relatório salvo.
4. Clique em **OK**, que atualiza o diálogo e mostra que o relatório foi salvo com sucesso.
5. Clique no botão**Fechar**para sair da janela de diálogo.

   O relatório salvo aparece sob **Meus Filtros** na seção de **Meus Conteúdos** da Central do Cliente.

Editando Filtros de Relatório Salvos

Para editar um filtro de relatório salvo:

1. Entre na Central do Cliente e abra o relatório desejado, seguindo a tarefa "Executando Relatórios" na página 138.
2. Na página Relatórios ou no painel de navegação, clique no link **Meus Conteúdos**.

3. Na página Meus Conteúdos ou no painel de navegação, clique no link **Meus Filtros**. A página Meus Filtros é aberta e mostra uma lista de filtros salvos.
4. Clique no nome de **Filtro** desejado para selecioná-lo. A página de relatórios se abre, exibindo os filtros que você salvou. Para mais informações, consulte "Salvando Filtros de Relatório" na página 149.
5. Edite os filtros existentes, conforme necessário, e faça uma das seguintes ações:
   - Para atualizar o filtro de relatórios existente, clique em **Mostrar resultados**. As alterações são salvas no filtro de relatório.
   - Para criar um novo filtro de relatório salvo:
     i) No cabeçalho do relatório, clique em .
     ii) No diálogo de Salvar Filtro de Relatório, digite um nome (até 48 caracteres) para o relatório e clique em **OK**.

     Um novo filtro de relatório salvo será criado e o filtro de relatório salvo original permanece inalterado.

Baixando Relatórios

Os usuários podem baixar qualquer relatório, inteiro ou em parte, da Central do Cliente. As solicitações para baixar relatórios são enfileiradas e processadas offline. Quando processados, os downloads de relatórios são disponibilizados na página Meus Relatórios. É possível baixar os dados de relatório nos formatos CSV (valores separados por vírgulas) ou XML (eXtensible Markup Language).

Baixando um relatório normalmente fornece mais informações na grelha de resultados do que visualizando o mesmo relatório na tela.

Para baixar um relatório:

1. Entre na Central do Cliente e abra o relatório desejado, seguindo a tarefa "Executando Relatórios" na página 138.
2. Em qualquer página de relatório, defina quaisquer filtros apropriados.
3. Clique em **Mostrar Resultados**.
4. Quando o relatório for mostrado, clique em .
5. Digite um nome para o relatório no campo **Nome de Relatório**.
6. Na lista **Formato de Relatório** selecione um valor **(CSV** ou **XML**).

   Não se esqueça, se você planeia carregar o relatório, só pode fazê-lo com um arquivo CSV.
7. Caso deseje receber uma notificação por e-mail quando o download estiver disponível, digite seu endereço de email no campo**Criar Alerta de Email**.
8. Clique no botão **Continuar** para colocar o download em fila.

   Quando a sua solicitação for processada, você pode recuperar o arquivo do relatório na página **Meus Relatórios**.

Para recuperar um relatório que foi processado:

1. No painel de navegação, clique no link **Meus Conteúdos** > **Meus Relatórios**.
2. Na página Meus Relatórios, na coluna **Status** clique no link de **Pronto**.

3. Siga as instruções fornecidas na tela para baixar o arquivo.

NOTA Enquanto a sua solicitação está sendo processada, a coluna **Status** exibe **Enfileirada** e o relatório não está disponível. Quando o processamento estiver concluído, a coluna de **Status** mostra o link **Pronto** e, se configurada para assim fazer, a Central do Cliente envia uma notificação por e-mail.

Segurança Multinível

Os recursos de segurança multi-nível da Central do Cliente permitem que um usuário autorizado conceda diferentes direitos e privilégios de acesso sobre relatórios a usuários ou grupos de usuários específicos. Existem cinco níveis diferentes de acesso de usuário: Administrador de Segurança, Administrador, Usuário de Segurança Avançado, Usuário Avançado e Convidado.

Para informações sobre contas de usuário, consulte "Usuários" na página 95. Para mais informações sobre os direitos de acesso e restrições de cada uma das funções de usuário, consulte "Funções de usuário e seus direitos de acesso" na página 96.

Capítulo 5: Trabalhando com Relatórios

Relatórios da Central do Cliente ajudam-lhe a rastrear e gerenciar seus ativos, permitindo que você reveja muitos tipos de informação, tais como:

- Datas Limite da Concessão
- Requisitos do Hardware
- Requisitos do Software
- Status da Licença do Software
- Atualizações necessárias

Os âmbitos dos relatórios da Central do Cliente variam muito. Alguns relatórios são amplos e incluem um resumo dos vários ativos, enquanto outros se concentram e especificam detalhes minuciosos que pertencem a um único dispositivo. Cada relatório da Central do Cliente é descrito neste capítulo.

NOTA Depois de um dispositivo ser sinalizado como Furtado, você pode vê-lo apenas em um relatório de ativos.

Este capítulo inclui as seguintes seções:

Níveis de Serviço e Relatórios

Os relatórios da Central do Cliente disponíveis para você dependem do nível de serviço que você adquiriu. Os relatórios do Computrace® Plus são disponibilizados a todos os clientes. Os clientes do Computrace® Plus não têm acesso aos relatórios avançados do Secure Asset Tracking™ e não estão qualificados para receber a Garantia de Serviço.

NOTA Para saber mais sobre como comprar, entre em contato com o departamento de vendas em:sales@absolute.com. Para informações sobre aquisições do Computrace® One™ entre em contato com o departamento de vendas EMEA da Absolute Software em sales@EMEA.absolute.com. Para obter informações de contato completas, consulte "Contatando o Suporte Global da Absolute Software" na página 23.

Para informações sobre os vários produtos Computrace e os relatórios da Central do Cliente que estão disponíveis para cada produto em cada plataforma suportada, vá para www.absolute.com/en/resources/matrices/absolute-computrace.

Relatórios de Ativos de Hardware

Os relatórios que aparecem na página Ativos de Hardware são determinados pelo nível de serviço que você adquiriu e podem incluir o seguinte:

- Relatório de Ativos
- Relatório de Impressora
- Relatório do Monitor
- Relatório de configurações do hardware e de alterações do SO
- Relatório do Espaço em Disco Rígido
- Relatório de Prontidão do Dispositivo
- Relatório de Adaptador de Banda Larga Móvel
- Relatório de Dispositivo Móvel

Relatório de Ativos

O Relatório de Ativos mostra todos os dispositivos de sua empresa que têm o Computrace agente instalado. O relatório mostra uma lista de dispositivos organizados em ordem crescente por Identificador. É possível personalizar o relatório para mostrar um subconjunto de dispositivos que atenda a critérios tais como para mostrar uma lista de todos os dispositivos em um departamento particular.

Para dispositivos com Windows Mobile, o relatório de Ativos exibe um subconjunto de informações.

NOTA Por padrão, o relatório de Ativos exibe os dispositivos dormentes. Para excluir dispositivos dormentes, desmarque a caixa de seleção **Incluir Dispositivos Dormentes** situada na parte inferior da área dos **Critérios de Pesquisa**.

Ao detectar números de série de discos rígidos, o agente Computrace consulta o controlador de disco em primeiro lugar. Se isso falhar, então o agente usa a Interface de Gerenciamento do Windows da Microsoft (WMI) para obter os números de série dos discos rígidos. Seja o que for que a WMI relatar, que é fornecido pela Microsoft ou pelo seu fornecedor de hardware e/ou de software, o mesmo aparece no Relatório de Ativos que foi baixado.

Para gerar um Relatório de Ativos:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Hardware** > **Relatório de Ativos**.
3. Na página Relatório de Ativos, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar os resultados por grupos de dispositivos, no campo **Onde o grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.

- **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
- **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
- **Marca**: o fabricante de um dispositivo ou outro hardware.

NOTA Para todos os dispositivos Chrome, a marca é **Chromebook**.

- **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
- **Número de Série**: o número de série do dispositivo ou outro hardware.
- **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
- **Nome de Usuário Atribuído**: o nome de usuário atribuído ao dispositivo por um administrador de sistemas.
- **Endereço de e-mail**: o endereço de e-mail da pessoa associada com este dispositivo ou esta atividade.
- **Fornecedor do Contrato de Garantia**: o prestador de garantia para um dispositivo.
- Quaisquer **Campos Definidos pelo Usuário (CDU)** que você pode ter definido estão listados aqui e você pode usá-los para filtrar seu relatório. Um UDF é um atributo para um dispositivo que um usuário da Central do Cliente pode criar e editar.

Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.

- Para filtrar resultados por data:

i) Na área **e quando**, abra a lista e selecione uma das seguintes opções:

- **Chamada mais recente** para abrir um relatório que mostra aqueles dispositivos que fizeram sua última chamada dentro dos parâmetros de data que você selecionou.
- **Data de Início de Concessão** para abrir um relatório que mostra aqueles dispositivos cuja concessão teve início dentro dos parâmetros de data que você selecionou.
- **Data Final de Concessão** para abrir um relatório que mostra aqueles dispositivos cuja concessão terminou dentro dos parâmetros de data que você selecionou.
- **Data de Início do Contrato de Serviço** para abrir um relatório que mostra aqueles dispositivos cujo contrato de serviços teve início dentro dos parâmetros de data que você selecionou.
- **Data Final do Contrato de Serviço** para abrir um relatório que mostra aqueles dispositivos cujo contrato de serviços terminou dentro dos parâmetros de data que você selecionou.
- **Data de Início de Garantia** para abrir um relatório que mostra aqueles dispositivos cuja garantia teve início dentro dos parâmetros de data que você selecionou.
- **Data Final de Garantia** para abrir um relatório que mostra aqueles dispositivos cuja garantia terminou dentro dos parâmetros de data que você selecionou.
- **Data de Aquisição do Dispositivo** para abrir um relatório que mostra aqueles dispositivos que foram adquiridos dentro dos parâmetros de data que você selecionou.

- ○ Quaisquer **Campos Definidos pelo Usuário (CDU)** que você pode ter definido estão listados aqui e você pode usá-los para filtrar seu relatório. Um UDF é um atributo para um dispositivo que um usuário da Central do Cliente pode criar e editar. Selecione esta opção para abrir um relatório que mostra aqueles dispositivos que são apropriados à sua seleção.

ii) Faça uma das seguintes opções:

- ○ Clique na opção de **a qualquer hora** para executar um relatório que mostra a chamada mais recente, independentemente de quando a mesma foi realizada.
- ○ No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um grande intervalo de datas leva mais tempo para gerar resultados.
- ○ No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.

● Para filtrar resultados por tipo de agente e versão, na área **e o Agente**:

i) No campo **Tipo** abra a lista e selecione o tipo de agente desejado da seguinte forma:

- ○ **Qualquer Tipo** retorna um relatório que mostra dispositivos com todos os tipos de agente.
- ○ **Android** retorna um relatório que mostra apenas dispositivos Android.
- ○ **BlackBerry** retorna um relatório que mostra apenas dispositivos BlackBerry.
- ○ **Chromebook** retorna um relatório que mostra apenas dispositivos Chrome para clientes com Computrace Mobile Theft Management (MTM). Para mais informações, consulte "Computrace Mobile Theft Management Mobile Theft Management para Dispositivos Chrome" na página 361.
- ○ **iOS** retorna um relatório que mostra apenas dispositivos iPad e iPad mini para clientes com Computrace Mobile Theft Management (MTM). Para mais informações, consulte "Computrace Mobile Theft Management para dispositivos iPad" na página 345.
- ○ **Mac** retorna um relatório que mostra apenas dispositivos Mac.
- ○ **Windows** retorna um relatório que mostra apenas dispositivos que rodam o sistema operacional Windows.
- ○ **Windows Mobile** retorna um relatório que mostra apenas dispositivos Windows Mobile.

ii) No campo **e versão**, abra a lista e selecione a **Versão** de agente desejada para o **Tipo** de agente que você selecionou anteriormente.

Por exemplo, se você deseja mostrar todos os dispositivos que possuem a versão 898 do agente instalado neles, no campo **tipo**, abra a lista e selecione **Qualquer Tipo** e no campo **versão** abra a lista e selecione **898**.

NOTA **SHC** (Chamada de Auto-Reparação) retorna um relatório que mostra dispositivos com agentes que chamaram como resultado de Persistência. Esta opção aparece quando uma chamada de auto-reparação ocorreu.

● Para filtrar os resultados por Departamento, no campo **e o Departamento é**, abra a lista e selecione o departamento desejado.

- Para filtrar os resultados por status de agente, no campo **e o Status de Agente é**, abra a lista e selecione:
  - **Ativo** mostra apenas aqueles dispositivos cujo agente chamou para o Centro de Monitoramento.
  - **Inativo** mostra apenas aqueles dispositivos cujo agente ainda não chamou para o Centro de Monitoramento.
  - **Desativado** mostra apenas aqueles dispositivos cujo agente está sinalizado para remoção ou removido do dispositivo.
- Na área **Exibir Resultados**, selecione uma ou mais das seguintes opções:
  - **Com campos definidos pelo usuário** para ver a informação que está relacionada com quaisquer campos definidos pelo usuário que você definiu.
  - **Incluir Dispositivos Inativos** para ver a informação para dispositivos dormentes que estão incluídos neste relatório por padrão. Se você não deseja exibi-los, desmarque esta caixa de seleção. Para mais informações sobre dispositivos dormentes, consulte "Usando o campo de Dispositivos Dormentes" na página 148.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.

   - Link para **Ver Histórico de Chamadas**, que você pode clicar para abrir o relatório do histórico de chamadas deste dispositivo. Na área de filtragem do Relatório do Histórico de Chamadas, os seguintes campos estarão preenchidos:
     - A área **e o campo** mostra o **Identificador** que você selecionou.
     - O campo **contém ou continha** mostra o dispositivo cujo link para **Ver Histórico de Chamadas** você clicou. Você pode continuar a filtrar de acordo com as informações na tarefa, "Relatório do Histórico de Chamadas" na página 208.
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Endereço de e-mail**: o endereço de e-mail da pessoa associada com este dispositivo ou esta atividade.
   - **Última Chamada**: a data e a hora quando o agente instalado no dispositivo mais recentemente contatou o Centro de Monitoramento.

     NOTA Para dispositivos Chrome, esta coluna mostra a data e a hora em que as informações de dispositivo na Central do Cliente foram sincronizadas com as informações de dispositivo na sua conta do Google.

   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Sistema Operacional**: o software que controla a execução de programas de computador e que pode prestar vários serviços.
   - **Versão do Agente**: o número de versão do agente que contata o Centro de Monitoramento.

NOTA Para dispositivos Chrome, este campo mostra **22xx** se o dispositivo não tiver sido furtado. Se o dispositivo tiver sido furtado, e o pacote Chrome MTM Deployment estiver implantado no dispositivo, o campo mostra **23*xx***. Para mais informações, consulte "Computrace Mobile Theft Management Mobile Theft Management para Dispositivos Chrome" na página 361.

- **Número de Série**: o número de série deste dispositivo.
- **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
- **Marca**: o fabricante deste dispositivo ou outro hardware.

NOTA Para todos os dispositivos Chrome, a marca é **Chromebook**.

- **Modelo**: o tipo de produto deste dispositivo ou outro hardware.
- **Departamento:** o departamento a que pertence este dispositivo.
- **Status do Agente**: a condição de operação do agente neste dispositivo, que poderá ser **Ativo**, **Inativo**, ou **Desativado**.
- **Nome de Usuário Atribuído**: o nome de usuário a que este dispositivo está atribuído.
- **Data do Furto**: se um relatório de furto aberto exisitir para este dispositivo, a data e a hora que indicam quando foi percebido que o dispositivo estava em falta.

Relatório de Impressora

O Relatório de Impressora não exibe dados na tela. Em vez disso, o relatório de impressora permite que os usuários façam o download de um arquivo CSV (valores separados por vírgula) ou XML (eXtensible Markup Language) que identifica os drivers de impressoras instaladas, as portas de impressora e dispositivos por impressora.

Para gerar um Relatório de Impressora:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Hardware** > **Relatório de Impressora**.
3. Na página Relatório de Impressora, na área **Critérios de Pesquisa**, defina as opções de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - No campo **Exibir**, selecione uma das seguintes opções:
     - **Drivers de Impressora** retorna um arquivo CSV ou XML que organiza os dados de drivers de impressoras de acordo com o nome do driver da impressora. O driver de impressora pode fornecer informações importantes para resolução de problemas pelo suporte técnico.
       Os arquivos CSV ou XML de drivers incluem as seguintes colunas:
       – **Nome do Servidor**: o servidor que hospeda a impressora.
       – **Nome do Compartilhamento**: o nome da rede da impressora.
       – **Driver da Impressora**: O nome do driver da impressora.
       – **Nome da Impressora**: o nome da impressora.
       – **Porta**: a porta sob qual a impressora opera.

- **Atributo**: indica se a impressora está instalada localmente ou em uma rede como uma impressora compartilhada.

  - **Portas de Impressora** retorna um arquivo CSV ou XML que organiza os dados do driver da impressora de acordo com a sua porta.

    Os arquivos CSV ou XML de portas de impressoras incluem as seguintes colunas:

    - **Porta**: a porta sob qual a impressora opera.
    - **Nome do Servidor**: o servidor que hospeda a impressora.
    - **Nome do Compartilhamento**: o nome da rede da impressora.
    - **Driver da Impressora**: O nome do driver da impressora.
    - **Nome da Impressora**: o nome da impressora.
    - **Atributo**: indica se a impressora está instalada localmente ou através de compartilhamento de rede.

  - **Dispositivos por Impressora** retorna um arquivo CSV ou XML que lista todos os dispositivos com drivers de impressora instalados.

    Quando os critérios do relatório são definidos para este valor, a página se atualiza e inclui **o campo o Grupo é**. Para filtrar os resultados por grupo de dispositivos, abra a lista e selecione o grupo de dispositivos desejado.

    Os arquivos CSV ou XML de dispositivos por impressoras incluirão as seguintes colunas:

    - **Nome do Servidor**: o servidor que hospeda a impressora.
    - **Nome do Compartilhamento**: o nome da rede da impressora.
    - **Driver da Impressora**: O nome do driver da impressora.
    - **Nome da Impressora**: o nome da impressora.
    - **Atributo**: indica se a impressora está instalada localmente ou através de compartilhamento de rede.
    - **Identificador**: o número de identificação única associado ao dispositivo.
    - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
    - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
    - **Departamento**: o departamento ao qual o dispositivo pertence.

- No campo **o Grupo é**, abra a lista para mostrar todos os Grupos de Dispositivos em sua conta e selecione **Todos os Dispositivos** ou o **Nome do Grupo de Dispositivos** desejado.

4. Na área de **Nome e Formato**, no campo **Nome**, digite um nome único para seu relatório.
5. No campo **Formato**, abra a lista e selecione uma das seguintes opções:
   - **CSV**: um arquivo de texto simples com colunas separadas por vírgula que é aberto com software incluído no seu sistema operacional. Recomendado para consultas SQL e o carregamento de arquivos de dados grandes.
   - **XML:** um arquivo de linguagem que é aberta com um editor de XML, tal como o Microsoft Excel ou OpenOffice. Recomendado para a filtragem e a formatação de dados.
6. No local de Criar Alerta de E-mail, no campo **Seu Endereço de E-mail**, digite seu endereço de e-mail se você deseja receber uma notificação por e-mail quando o relatório estiver processado.
7. Clique no botão **Continuar** para colocar o download em fila.

8. Quando sua solicitação for processada, você pode obter o arquivo CSV ou XML do relatório na página **Meus Relatórios**. Para mais informações, consulte "Baixando Relatórios" na página 150.

Relatório do Monitor

O Relatório de Monitores não exibe dados na tela. Em vez disso, o relatório de monitores permite que os usuários façam o download de um arquivo CSV (Comma Separated Value) ou XML (eXtensible Markup Language) que identifica os drivers de monitores instalados.

Para gerar um Relatório de Monitor:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Hardware** > **Relatório de Monitor**.
3. Na página Relatório de Monitores, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar os resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar resultados por dispositivo específico, abra a lista **e o campo** e selecione um dos seguintes valores:
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
     - **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
     - **Número de Série**: o número de série do dispositivo ou outro hardware.
     - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
     - **Departamento:** o departamento a que pertence este dispositivo.
     - **Marca**: o fabricante de um dispositivo ou outro hardware.
     - **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
     - **Fabricante do Monitor:** o fabricante do monitor do dispositivo.
     - **Tipo de Monitor**: a configuração do monitor tal como Padrão ou Plug and Play.
     - **Frequência de atualização do monitor**: o número de vezes em um segundo que um monitor desenha os dados. O aumento da taxa de atualização pode diminuir a cintilação e reduzir tensão ocular.
     - **Descrição do dispositivo de vídeo**: o nome da placa de vídeo do dispositivo.
     - **Resolução do monitor de vídeo**: o número de pixels distintos que podem ser exibidos pelo monitor citado como largura x altura, com as unidades em pixels tal como 1024 x 768.
     - **Intensidade de cor da exibição de vídeo**: o número de bits usados para indicar a cor de um único pixel em uma imagem de bitmap ou vídeo, tal como monocromático de 1 bit ou tons de cinzento de 8 bits.

   Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.
4. Na área de **Nome e Formato**, no campo **Nome**, digite um nome único para seu relatório.

5. No campo **Formato**, abra a lista e selecione uma das seguintes opções:
   - **CSV**: um arquivo de texto simples com colunas separadas por vírgula que é aberto com software incluído no seu sistema operacional. Recomendado para consultas SQL e o carregamento de arquivos de dados grandes.
   - **XML:** um arquivo de linguagem que é aberta com um editor de XML, tal como o Microsoft Excel ou OpenOffice. Recomendado para a filtragem e a formatação de dados.
6. No local **Criar Alerta de E-mail**, no campo **Seu Endereço de E-mail**, digite seu endereço de e-mail se você deseja receber uma notificação por e-mail quando o relatório estiver processado.
7. Clique no botão **Continuar** para colocar o download em fila.
8. Quando sua solicitação for processada, você pode obter o arquivo CSV ou XML do relatório na página **Meus Relatórios**. Para mais informações, consulte "Baixando Relatórios" na página 150.

NOTA Se um dispositivo monitorado usar um driver genérico para o monitor ou placa de vídeo, alguns valores do Relatório do Monitor podem ser registrados e mostrados como **Tipo de Monitor Padrão**, **Monitor Plug and Play**, **Monitor Genérico**, ou **Monitor Padrão**.

Relatório de configurações do hardware e de alterações do SO

O Relatório de configurações do hardware e de alterações do SO identifica todos os ativos que sofrem alterações ao seu hardware crítico ou ao sistema operacional (SO) durante o período de tempo que você define. Veja a coluna **Descrição de Hardware** para detalhes sobre quais as alterações que foram detectadas no hardware (tais como placas de rede) e no sistema operacional.

Ao detectar números de série de discos rígidos, o agente Computrace consulta o controlador de disco em primeiro lugar. Se isso falhar, então o agente usa a Interface de Gerenciamento do Windows da Microsoft (WMI) para obter os números de série dos discos rígidos. Seja o que for que a WMI relatar, que é fornecido pela Microsoft ou pelo seu fornecedor de hardware e/ou de software, o mesmo aparece no Relatório de Configurações de Hardware e de Alterações do SO.

Para gerar um Relatório de Configurações do Hardware e de Alterações ao SO:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Hardware** > **Relatório de Configurações do Hardware e de Alterações ao Sistema Operacional**.
3. Na página Configuração de Hardware e Alteração do Sistema Operacional, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar os resultados por grupos de dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Identificador**: um número de série eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.

- Quaisquer **Campos Definidos pelo Usuário (CDU)** que você pode ter definido estão listados aqui e você pode usá-los para filtrar seu relatório. Um UDF é um atributo para um dispositivo que um usuário da Central do Cliente pode criar e editar.

  Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.

- Para filtrar seus resultados por Departamento, no campo **e o Departamento**, abra a lista e selecione o departamento desejado.
- Para filtrar seus resultados pela data em que a alteração ocorreu, na área **e a alteração ocorreu entre**, faça uma das seguintes ações:
  - No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados.
  - No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.
- Para filtrar seus resultados pelo status da alteração ao **hardware ou ao sistema operacional**, na área de **Status**, selecione uma das seguintes opções:
  - **Mostrar Todas as Alterações**: retorna um relatório que mostra o hardware e o sistema operacional que foi instalado, removido ou reconfigurado em um dispositivo.
  - **Mostrar apenas as Alterações**: retorna um relatório que mostra o hardware ou sistema operacional que foi reconfigurado em um dispositivo.
  - **Mostrar apenas os Removidos**: retorna um relatório que mostra o hardware ou sistema operacional que foi desinstalado em um dispositivo.
  - **Mostrar apenas os Novos**: retorna um relatório que mostra o hardware ou sistema operacional que foi substituído em um dispositivo.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem:
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Descrição de Hardware**: o hardware ou sistema operacional que foi alterado.
   - **Data Detectada**: a data e a hora quando a alteração foi detectada.
   - **Anterior:** a descrição do hardware ou sistema operacional anterior.
   - **Novo:** a descrição do hardware ou sistema operacional atual.
   - **Status**: indica se uma diferença detectada envolve software ou hardware Novo, Removido ou Alterado.

Relatório do Espaço em Disco Rígido

O relatório de Espaço em Disco Rígido mostra o espaço total, usado e disponível nos discos rígidos de cada volume de disco detectado em dispositivos rastreados. A coleção de dados usando este relatório permite que você rastreie dispositivos que podem não ser capazes de aceitar atualizações de software ou que estejam sem espaço disponível no disco rígido.

Para gerar um relatório do Espaço em Disco Rígido:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Hardware** > **Relatório de Espaço em Disco Rígido**.
3. Na Relatório do Espaço em Disco Rígido, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar os resultados por grupos de dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Quaisquer dos campos nesta lista**: seleciona todos os valores na lista.
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
     - Quaisquer **Campos Definidos pelo Usuário (CDU)** que você pode ter definido estão listados aqui e você pode usá-los para filtrar seu relatório. Um UDF é um atributo para um dispositivo que um usuário da Central do Cliente pode criar e editar.

     Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento**, abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados pela quantidade de espaço disponível no disco rígido do dispositivo, na área **e qualquer Volume tem menos de**, faça uma das seguintes ações:
     - Abra a lista e selecione um valor para o espaço disponível no disco rígido.
     - Na parte inferior do painel dos Critérios de Pesquisa, selecione a caixa de seleção **Exibir tamanho de disco rígido e espaço disponível para todos os dispositivos selecionados** para mostrar todos os dispositivos com menos de 100% de espaço disponível no disco rígido.
4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem. Algumas das colunas no relatório podem não estar visíveis na sua tela. Para visualizar todas as colunas em um relatório, use a seta no seu teclado para rolar para a direita.
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.

- **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
- **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
- **Endereço de e-mail**: o endereço de e-mail da pessoa associada com este dispositivo ou esta atividade.
- **Valor do Limite (MB)**: a quantidade mínima de espaço disponível no disco rígido necessitada pelo sistema operacional para funcionar antes de afetar o desempenho de seu desempenho. Se o valor na coluna Espaço livre no Volume é inferior ao Valor do Limite, seu dispositivo pode correr o risco de se desligar.
- **Volume**: uma partição de espaço de armazenamento no disco rígido identificada por uma letra, tal como `A:\` ou `B:\`.
- **Etiqueta de Volume**: o nome descritivo atribuído a um volume em um disco rígido, tal como Disco Local ou Público.
- **Tamanho do Volume (MB)**: a capacidade de armazenamento do volume, em megabytes (MB).
- **Espaço Livre no Volume (MB)**: o espaço para armazenamento disponível no volume em megabytes (MBs).
- **Espaço Usado no Volume (MB)**: o espaço para armazenamento usado no volume em megabytes (MBs).
- **Tamanho do Disco Rígido (MB)**: o espaço para armazenamento total no dispositivo em megabytes (MBs).
- **Espaço Livre em Disco Rígido (MB)**: o espaço para armazenamento disponível no disco rígido em megabytes (MBs).
- **Espaço Utilizado do Disco Rígido (MB)**: o espaço para armazenamento utilizado no disco rígido em megabytes (MBs).

Relatório de Prontidão do Dispositivo

O relatório de Prontidão do Dispositivo identifica dispositivos que não atendem aos valores mínimos de requisitos de componentes de hardware ou de sistema operacional especificados pelo usuário.

O Relatório de Prontidão do Dispositivo permite que você faça o seguinte:

- Localizar dispositivos que não são compatíveis com um determinado software ou lançamento de sistema operacional.
- Localizar dispositivos que estão prontos para desativação.
- Identificar componentes de hardware que requerem uma atualização.

O relatório padrão é gerado usando um sistema operacional (SO) específico, que você pode escolher de uma lista, e as seguintes especificações mínimas de hardware:

- Velocidade da CPU maior que 300 MHz
- RAM maior que 128 MB
- O tamanho do disco rígido é maior que 2 GB
- Espaço livre em disco rígido maior que 1,5 GB

O Relatório de Prontidão de Dispositivos mostra todos os dispositivos que não atendam a quaisquer ou a nenhum dos requisitos definidos, agrupados de acordo com os critérios que os dispositivos falharam em atender.

Para gerar um Relatório de Prontidão de Dispositivos:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Hardware** > **Relatório de Prontidão de Dispositivos**.
3. Na **página Relatório de Prontidão de Dispositivos**, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar os resultados por grupos de dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento**, abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Marca**: o fabricante de um dispositivo ou outro hardware.

       NOTA Para todos os dispositivos Chrome, a marca é **Chromebook**.

     - **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
     - Quaisquer **Campos Definidos pelo Usuário (CDU)** que você pode ter definido estão listados aqui e você pode usá-los para filtrar seu relatório. Um UDF é um atributo para um dispositivo que um usuário da Central do Cliente pode criar e editar.

   Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.
4. Na área dos requisitos do sistema, para aplicar condições aos resultados de seu relatório, faça o seguinte:
   - Para definir as condições do relatório, selecione uma das seguintes opções:
     - **Qualquer**: mostra dispositivos que atendem aos requisitos padrão do sistema.
     - **Todas as seguintes condições são verdadeiras**: mostra dispositivos que atendem aos requisitos do sistema que você inseriu.
   - Selecione a caixa de seleção **O/S** para filtrar seus resultados por Sistema Operacional.
     i) Abra a lista e selecione uma das seguintes opções:
        - **É** mostra dispositivos que possuem o sistema operacional selecionado.
        - **Não é** exclui dispositivos que possuem o sistema operacional selecionado.

     ii) Clique em**Escolher**. No diálogo Escolher, clique **>** para adicionar o campo ao painel dos Campos Selecionados. Para adicionar todos os campos, clique em **>>**.

     iii) Para remover um campo, selecione o campo no painel Campos Selecionados , e em seguida clique **<.** Para remover todos os campos, clique em **<<**.
   - Marque a caixa de seleção **CPU** para filtrar seus resultados por um tipo de processador específico.
     i) Abra a lista e selecione uma das seguintes opções:
        - **É** mostra dispositivos que possuem o CPU que você selecionou.
        - **Não É** exclui dispositivos que possuem o CPU que você selecionou.

ii) Clique em**Escolher**. No diálogo Escolher, clique **>** para adicionar o campo ao painel dos Campos Selecionados. Para adicionar todos os campos, clique em **>>**.

iii) Para remover um campo, selecione o campo no painel Campos Selecionados , e em seguida clique **<.** Para remover todos os campos, clique em **<<**.

- Para filtrar seus resultados por uma velocidade de processador específica, na área de **CPU Max Detectada**:

  i) Abra a lista e selecione uma das seguintes opções:

    - **<**: para um valor que é menor que.
    - **<=:** para um valor que é menor que ou igual a.
    - **=**: para um valor que iguala.
    - **>=**: para um valor que é maior que ou igual a.
    - **>**: para um valor que é maior que.

  ii) No campo **MHz**, insira um valor para a velocidade do processador.

- Para filtrar seus resultados por uma velocidade de memória específica, na área de **RAM**:

  i) Abra a lista e selecione uma das seguintes opções:

    - **<**: para um valor que é menor que.
    - **<=:** para um valor que é menor que ou igual a.
    - **=**: para um valor que iguala.
    - **>=**: para um valor que é maior que ou igual a.
    - **>**: para um valor que é maior que.

  ii) No campo **MB**, insira um valor para a velocidade da memória do dispositivo.

- Para filtrar seus resultados por um tamanho de disco rígido, na área de **Tamanho do Disco Rígido**:

  i) Abra a lista e selecione uma das seguintes opções:

    - **<**: para um valor que é menor que.
    - **<=:** para um valor que é menor que ou igual a.
    - **=**: para um valor que iguala.
    - **>=**: para um valor que é maior que ou igual a.
    - **>**: para um valor que é maior que.

  ii) No campo **MB**, insira um valor para o tamanho do disco rígido do dispositivo.

- Para filtrar resultados pela quantidade de espaço livre no disco rígido, na área de **Espaço Livre no Disco Rígido**:

  i) Abra a lista e selecione uma das seguintes opções:

    - **<**: para um valor que é menor que.
    - **<=:** para um valor que é menor que ou igual a.
    - **=**: para um valor que iguala.
    - **>=**: para um valor que é maior que ou igual a.
    - **>**: para um valor que é maior que.

  ii) No campo **MB**, insira um valor para a quantidade de espaço livre no disco rígido do dispositivo.

5. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Sistema Operacional**: software que controla a execução de programas de computador e que pode prestar vários serviços.
   - **Nome da CPU:** o fabricante da Unidade de Processamento Central.
   - **Velocidade da CPU:** a velocidade de processamento da Unidade de Processamento Central.
   - **Tamanho da RAM**: a quantidade de Memória de Acesso Aleatório (RAM) no dispositivo.
   - **Tamanho do Disco Rígido**: o armazenamento de dados disponível no dispositivo em megabytes (MBs).
   - **Espaço Livre em Disco Rígido:** o espaço para armazenamento disponível no disco rígido em megabytes (MBs).
   - **Marca**: o fabricante de um dispositivo ou outro hardware.

     NOTA Para todos os dispositivos Chrome, a marca é **Chromebook**.

   - **Modelo**: o tipo de produto de um dispositivo ou outro hardware.

Relatório de Adaptador de Banda Larga Móvel

IMPORTANTE Antes de usar o recurso de Tecnologia de Tempo Real (Real Time Technology - RTT), incluindo o rastreamento de ativos de Adaptadores de Banda Larga Móvel e Chamadas Iniciadas pelo Centro de Monitoramento, você precisa ativar esses recursos para a sua conta ou identificadores individuais dentro da sua conta. Entre em contato com o Suporte Global da Absolute Software para ativar estes recursos. Para mais informações sobre como entrar em contato com o suporte, consulte "Contatando o Suporte Global da Absolute Software" na página 23.

O relatório de Adaptadores de Banda Larga Móvel mostra uma lista de adaptadores de banda larga móvel, também conhecidos como modems celulares, instalados e funcionando em dispositivos gerenciados.

As informações que aparecem no relatório de Adaptadores de Banda Larga Móvel também estão disponíveis na página Resumos de Dispositivos para um dispositivo específico. Para mais informações, consulte "Editando Informações de Ativos" na página 141.

Para gerar um Relatório de Adaptadores de Banda Larga Móvel:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Hardware** > **Relatório de Adaptadores de Banda Larga Móvel**.

3. Na **página Relatório de Adaptadores de Banda Larga Móvel**, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização para o relatório, usando um ou mais dos seguintes critérios:

   - Para filtrar os resultados por grupos de dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Quaisquer dos campos nesta lista**: seleciona todos os valores na lista.
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Fabricante do Adaptador de Banda Larga Móvel**: o nome do fabricante do adaptador de banda larga móvel.
     - **Modelo do Adaptador de Banda Larga Móvel**: o número de modelo, se disponível, do adaptador de banda larga móvel.
     - **ID do Equipamento do Adaptador de Banda Larga Móvel**: o número de identificação do adaptador.
     - **ID do Assinante de Adaptador de Banda Larga Móvel**: o número único associado ao assinante; armazenado no adaptador, o chip Módulo de Identidade do Assinante (SIM) ou equivalente.
     - **Rede do Adaptador de Banda Larga Móvel**: o fornecedor de serviço móvel associado ao adaptador de banda larga móvel.
     - **Qualquer Número do Telefone**: o número de telefone detectado ou o número de telefone substituto associado ao dispositivo móvel.
     - **Número de Telefone Detectado**: o número de telefone associado ao adaptador de banda larga móvel, como relatado pelo dispositivo.
     - **Número de Telefone Substituto**: o número de telefone alternativo ou substituto associado ao dispositivo móvel ou ao adaptador de banda larga fornecido por um administrador quando um número de telefone não é automaticamente detectado.

     Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento**, abra a lista e selecione o departamento desejado.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.

   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome de Usuário do Dispositivo**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Marca do Dispositivo**: o fabricante do dispositivo móvel.
   - **Modelo do Dispositivo**: o tipo de produto do dispositivo móvel.
   - **Adaptador Detectado pela Última Vez**: a data e a hora quando o adaptador instalado no dispositivo mais recentemente contatou o Centro de Monitoramento.

- **Fabricante do Adaptador**: o nome da empresa que fabricou o adaptador de banda larga móvel.
- **Modelo do Adaptador**: o tipo de produto de um adaptador de rede de banda larga móvel.
- **ID do Equipamento**: o número de identificação único de um smartphone. A ID do equipamento é tipicamente encontrado em uma etiqueta impressa na bateria. Para smartphones CDMA, o Número de Série Eletrônico (ESN) ou a ID de Equipamento Móvel (MEID) são relatados. Para smartphones GSM e UMTS, a Identificação Internacional de Equipamento Móvel (IMEI) é relatada.
- **ID do Assinante**: o número único associado ao assinante do serviço de rede do smartphone. O número é obtido a partir do hardware do smartphone, do cartão do Módulo de Identidade do Assinante (SIM), ou um equivalente.
- **Rede**: o fornecedor de serviço móvel associado ao adaptador de banda larga móvel.
- **Número do Telefone Detectado**: o número de telefone associado ao adaptador de banda larga móvel, como relatado pelo dispositivo.
- **Número de Telefone Substituto**: o número de telefone alternativo associado ao dispositivo móvel ou ao adaptador de banda larga. Se um número de telefone de um dispositivo não for automaticamente detectado, o dispositivo envia um SMS, também conhecido como mensagem de texto, ao Centro de Monitoramento.

  O endereço "Responder para" da mensagem de texto se torna no valor do campo **Número de Telefone Substituto**. É possível também especificar um número de telefone substituto na página do Resumo do Dispositivo. Ao enviar mensagens de texto para um dispositivo, o valor do campo **Número de Telefone Substituto** tem precedência sobre o valor do campo **Número de Telefone Detectado**.

Relatório de Dispositivo Móvel

O relatório do dispositivo móvel mostra uma lista de smartphones e tablets em uma conta. Um smartphone é um telefone celular que oferece recursos avançados, muitas vezes com funcionalidades de um computador, e oferece um bom aparelho de convergência entre um computador e um telefone móvel.

Smartphones que suportam mais de uma tecnologia de rede aparecem várias vezes no relatório. Em tais casos, as colunas de **Número de Telefone**, **ID do Equipamento** e de **ID do Assinante** possuem valores diferentes para cada tecnologia de rede detectada.

Para gerar um Relatório de Dispositivo Móvel:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Hardware** > **Relatório de Dispositivos Móveis**.
3. Na página **Relatório de Dispositivos Móveis**, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.

- **Marca**: o fabricante de um dispositivo ou outro hardware.
- **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
- **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
- **Sistema operacional**: software que controla a operação e os aplicativos do dispositivo móvel e que pode fornecer vários serviços.
- **Número de Telefone Detectado**: o número de telefone associado ao dispositivo móvel.
- **ID do equipamento**: o número de identificação único de um smartphone. A ID do equipamento é tipicamente encontrado em uma etiqueta impressa na bateria. Para smartphones CDMA, o Número de Série Eletrônico (ESN) ou a ID de Equipamento Móvel (MEID) são relatados. Para smartphones GSM e UMTS, a Identificação Internacional de Equipamento Móvel (IMEI) é relatada.
- **ID do Assinante**: o número único associado ao assinante do serviço de rede do smartphone. O número é obtido a partir do hardware do smartphone, do cartão do Módulo de Identidade do Assinante (SIM), ou um equivalente.
- **Endereços MAC**: um ou mais endereços de Controle de Acesso ao Meio (MAC) detectados no Smartphone, mais comumente endereços de MAC Wi-Fi. Algumas plataformas podem também ter um endereço MAC Ethernet e outros campos definidos pelo usuário.

Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.

- Para filtrar os resultados por sistema operacional, na área **e o Sistema Operacional é**, abra a lista e selecione o sistema operacional desejado, da seguinte forma.
  - **Windows Mobile** retorna um relatório que mostra apenas dispositivos que rodam o sistema operacional Windows Mobile.
  - **BlackBerry** retorna um relatório que mostra apenas dispositivos que rodam o sistema operacional Blackberry.
  - **Android** retorna um relatório que mostra apenas dispositivos que rodam o sistema operacional Android.
  - **iOS** retorna um relatório que mostra apenas dispositivos iPad e iPad mini para clientes com Computrace Mobile Theft Management (MTM). Para mais informações, consulte "Computrace Mobile Theft Management para dispositivos iPad" na página 345.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Hora da Última Chamada**: um link que mostra a data e a hora quando o dispositivo mais recentemente contatou o Centro de Monitoramento. Clicando neste link abre o Relatório do Histórico de Chamadas. Para mais informações, consulte "Relatório do Histórico de Chamadas" na página 208.
   - **Nome de Usuário**: o nome único que identifica a pessoa que está associada a este dispositivo móvel.
   - **Endereço de e-mail**: o endereço de e-mail da pessoa associada a este dispositivo móvel.
   - **Marca**: o fabricante do dispositivo móvel.

- **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
- **Sistema Operacional**: o software que controla a operação e os aplicativos do dispositivo móvel e que pode fornecer vários serviços.
- **Número de Telefone**: o número de telefone associado ao dispositivo.
- **ID do equipamento**: o número de identificação único de um smartphone. O **ID do Equipamento** se encontra em uma etiqueta impressa na bateria. Para smartphones CDMA, o Número de Série Eletrônico (ESN) ou a ID de Equipamento Móvel (MEID) são relatados. Para smartphones GSM e UMTS, a Identificação Internacional de Equipamento Móvel (IMEI) é relatada.
- **ID do Assinante**: o número único associado ao assinante do serviço de rede do smartphone. O número é obtido a partir do hardware do smartphone, do cartão do Módulo de Identidade do Assinante (SIM), ou um equivalente.
- **Endereços MAC**: indica que um ou mais endereços de Controle de Acesso ao Meio (MAC) foram detectados no smartphone, mais comumente endereços de MAC Wi-Fi. Algumas plataformas podem também ter um endereço MAC Ethernet.

Relatório de Ativos de Software

A capacidade do agente para identificar automaticamente os aplicativos instalados é prejudicada porque alguns desenvolvedores de software não aderem aos padrões publicados para a identificação de seus produtos. Geralmente, os desenvolvedores de aplicativos incorporam as informações de identificação no próprio código de seus produtos. Infelizmente, as informações não são incorporadas da mesma forma de uma empresa para outra ou, em alguns casos, de um produto para outro na mesma empresa.

Para atender ao problema causado por diferenças nas informações incorporadas, a Absolute Software mantém um banco de dados que distingue os aplicativos pela forma como as informações de identificação são registradas no aplicativo. Conforme o banco de dados se desenvolve, a capacidade do agente para identificar aplicativos específicos aumenta.

Os relatórios que aparecem na página Ativos de Software são determinados pelo nível de serviço que você adquiriu e todos os relatórios são descritos.

Esta seção fornece informações sobre tarefas relacionadas para os seguintes relatórios:

- Relatório da Visão Geral do Software Instalado
- Relatório da Alteração da Configuração de Software
- Relatório de Software por Dispositivo
- Relatório do Resumo Geral da Conformidade de Licença de Software
- Relatório de Dispositivos por Licença
- Relatório do Resumo de Auditoria da Microsoft
- Relatório da Não Conformidade com a Política de Software
- Relatório de Programas Instalados por Dispositivo
- Relatório de Programas Instalados por Conta

Relatório da Visão Geral do Software Instalado

O Relatório da Visão Geral de Software Instalado mostra aplicativos de software detectados em dispositivos rastreados. É possível usar o relatório para executar inventário de software e gerenciamento de licenças, assim como para identificar aplicativos de software essenciais ou não essenciais. Para informações sobre como disponibilizar mais aplicativos a partir deste relatório, consulte "Solicitando Novos Aplicativos de Software a Incluir no Relatório da Visão Geral de Software Instalado" na página 172.

O Relatório da Visão Geral de Software Instalado exibe um registro para cada executável que é detectado em um dispositivo. Este relatório é independente de licenças de software. Um aplicativo licenciado pode ter vários registros mostrados no relatório da Visão Geral de Software Instalado. Por exemplo, o Microsoft Office mostraria registros separados para o Word, Access, Excel e outros aplicativos do Office.

Por padrão, o Relatório da Visão Geral de Software Instalado exibe todos os títulos de softwares detectados em dispositivos gerenciados, organizados por nome do fornecedor. Este relatório exibe todos os dispositivos que atendem parte ou todos os requisitos definidos.

IMPORTANTE Não há informações disponíveis para identificar o **Editor** de um aplicativo em dispositivos com Windows Mobile. Portanto, se seus ativos incluem dispositivos com Windows Mobile, todos os softwares desses dispositivos serão agrupados como **Editor: (Nenhum)** e são mostrados na parte superior do relatório da Visão Geral de Software Instalado.

Para monitorar e rever detalhes de licenças de software, consulte "Relatório do Resumo Geral da Conformidade de Licença de Software" na página 176.

Para gerar um Relatório da Visão Geral de Software Instalado:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Software** > **Relatório do Resumo Geral de Software Instalado**.
3. Na página **Relatório** do Resumo Geral do Software Instalado, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por um Departamento, no campo **e o Departamento é** , abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados por um fornecedor de software, tal como a Microsoft ou a Adobe, na área **e o Fornecedor contém**:
     i) Digite todo ou parte do nome do editor de software.
     ii) Clique em **Escolher** e selecione o fornecedor desejado.
   - Para filtrar seus resultados por um nome de aplicativo específico, tal como o Microsoft Word ou Adobe Photoshop, na área **e o Nome do Aplicativo contém**:
     i) Digite todo ou parte do nome do aplicativo.
     ii) Clique em **Escolher** e selecione o aplicativo desejado.
   - Para filtrar seus resultados por um nome de programa específico, tal como o Microsoft Word ou Adobe Creative Suite, na área **e o Nome do Programa contém**:

i) Digite todo ou parte do nome do programa.
ii) Clique em **Escolher** e selecione o programa desejado.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.
   - **Fornecedor**: a empresa que criou o aplicativo de software.
   - **Nome do Aplicativo**: o nome do aplicativo no dispositivo e sua função, se disponível.
   - **Nome do Programa**: o título associado a um ou mais aplicativos relacionados. Na prática, muitos editores trocam mutuamente de valores de **Nomes de Aplicações** e **Nomes de Programas**.
   - **Versão**: um número que distingue lançamentos do mesmo aplicativo de software vendido separadamente, como detectado pelo agente e relatado na Central do Cliente.
   - **Contagem de Instalações**: o número de dispositivos que têm este programa instalado.

   IMPORTANTE A Central do Cliente não pode mostrar informações que não consegue encontrar. Na grelha de resultados, conteúdos em branco nos campos **Fornecedor**, **Aplicativo**, **Programa** ou **Versão** indicam que os vendedores não forneceram tal informação com seus programas.

Solicitando Novos Aplicativos de Software a Incluir no Relatório da Visão Geral de Software Instalado

A Absolute Software convida seus clientes a solicitarem aplicativos específicos que eles gostariam de inserir no banco de dados de aplicativos de software detectados, também conhecido como mapeamento de software.

Para solicitar que um aplicativo específico seja mapeado e incluído no relatório da visão geral de software instalado, envie sua solicitação de mapeamento de software ao Suporte Global da Absolute, como instruído na tarefa, "Contatando o Suporte Global da Absolute Software" na página 23.

Inclua as seguintes informações na sua solicitação ao Suporte Global:

- Nome do Aplicativo
- Versão do Programa
- Nome do Desenvolvedor
- Página Inicial do Desenvolvedor
- **Identificador**, **Nome de Dispositivo** e **Nome de Usuário**, ou **endereço de Email atribuído** de pelo menos um dispositivo onde o aplicativo esteja instalado, incluindo a data e hora de instalação

IMPORTANTE A Absolute Software não garante a implementação de todas as solicitações de mapeamento de software.

Relatório da Alteração da Configuração de Software

O Relatório da Alterações de Configuração de Software identifica todos os dispositivos em que algum software foi instalado, desinstalado ou atualizado durante um período de tempo especificado. Para atualizações, o relatório exibe os números da versão anterior e da nova versão.

NOTA A configuração padrão do Relatório de Alteração de Configuração de Software pode não apresentar resultados. Poderá ser necessário aumentar o intervalo de datas ou modificar outros filtros e gerar novamente o relatório.

Para gerar um Relatório da Alteração de Configuração de Software Instalado:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Software** > **Relatório da Alteração de Configuração de Software**.
3. Na **página Relatório da Alteração de Configuração de Software**, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Quaisquer dos campos nesta lista**: seleciona todos os valores na lista.
     - **Identificador**: um número de série eletrônico único atribuído ao agente instalado em um dispositivo
     - **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
     - Quaisquer **Campos Definidos pelo Usuário (CDU)** que você pode ter definido estão listados aqui e você pode usá-los para filtrar seu relatório. Um UDF é um atributo para um dispositivo que um usuário da Central do Cliente pode criar e editar.

     Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.
   - Para filtrar seus resultados por um Departamento, no **campo e o Departamento é** abra a lista e selecione o departamento apropriado.
   - Para filtrar seus resultados por um fornecedor de software, na área **e o Fornecedor contém**:
     i) Digite todo ou parte do nome do editor de software.
     ii) Clique em **Escolher** e selecione o fornecedor desejado.
   - Para filtrar seus resultados por um aplicativo específico, na área **e o Nome do Aplicativo contém**:
     i) Digite todo ou parte do nome do aplicativo.
     ii) Clique em **Escolher** e selecione o aplicativo desejado.
   - Para filtrar seus resultados por um programa específico, na área **e o Nome do Programa contém**:
     i) Digite todo ou parte do nome do aplicativo.
     ii) Clique em **Escolher** e selecione o programa desejado.
   - Para filtrar seus resultados pela data em que o agente detectou uma alteração, na área **e a alteração ocorreu entre**, faça uma das seguintes ações:

- No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados.
- No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.

- Para filtrar seus resultados pelo status da alteração à configuração de software do dispositivo, selecione uma das seguintes opções:
  - **Todos**: retorna um relatório que mostra todo o software que foi instalado, removido ou reconfigurado em um dispositivo.
  - **Alterado**: retorna um relatório que mostra o software que foi reconfigurado em um dispositivo.
  - **Novos**: retorna um relatório que mostra o software que foi instalado em um dispositivo.
  - **Removido**: retorna um relatório que mostra o software que foi desinstalado de um dispositivo.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.
   - Link para o **Identificador**, que você clica para abrir a página do Resumo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome de Usuário**: o nome único que identifica a pessoa que está associada a este dispositivo
   - **Fornecedor**: uma empresa ou organização que vende aplicativos que é detectada pelo agente e relatada na Central do Cliente.
   - **Nome do Aplicativo**: o nome do aplicativo no dispositivo e sua função, se disponível. Na prática, muitos fornecedores trocam mutuamente de valores de Nomes de Aplicações e Nomes de Programas.
   - **Nome do Programa**: o título associado a um ou mais aplicativos relacionados. Na prática, muitos fornecedores trocam mutuamente de valores de Nomes de Aplicações e Nomes de Programas.
   - **Versão Anterior**: o número da versão anterior da instalação de um programa.
   - **Nova Versão**: o número da versão atual da instalação de um programa.
   - **Alteração Detectada na Data**: a data quando o agente detectou uma alteração que foi feita à configuração de software do dispositivo.
   - **Status**: indica se uma diferença detectada envolve software **Novo**, **Removido** ou **Alterado**.

   IMPORTANTE A Central do Cliente não pode mostrar informações que não consegue encontrar. Na grelha de resultados, conteúdos em branco nos campos **Fornecedor**, **Aplicativo**, **Programa** ou **Versão** indicam que os vendedores não forneceram tal informação com seus programas.

Relatório de Software por Dispositivo

O Relatório de Software por Dispositivo mostra uma lista de todos os softwares detectados e instalados em cada dispositivo rastreado.

Para gerar um Relatório de Software por Dispositivo

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Software** > **Relatório de Software por Dispositivo**.
3. Na página Relatório de Software por Dispositivo, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Quaisquer dos campos nesta lista**: seleciona todos os valores na lista.
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
     - **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
     - Quaisquer **Campos Definidos pelo Usuário (CDU)** que você pode ter definido estão listados aqui e você pode usá-los para filtrar seu relatório. Um UDF é um atributo para um dispositivo que um usuário da Central do Cliente pode criar e editar.

   Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.
   - Para filtrar seus resultados por um Departamento, no **campo e o Departamento é** abra a lista e selecione o departamento apropriado.
   - Para filtrar resultados por software, na **área e o campo** , abra a lista e selecione um dos seguintes valores:
     - **Fornecedor**: a empresa que está desenvolvendo um aplicativo de software.
     - **Aplicativo**: o título de um arquivo executável.
     - **Versão**: um número que distingue lançamentos do mesmo aplicativo de software vendido separadamente, como detectado pelo agente e relatado na Central do Cliente.
     - **Programa**: um arquivo executável em um dispositivo que é detectado pelo agente e relatado na Central do Cliente.

   Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.
4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem:
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Departamento:** o departamento a que pertence este dispositivo.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.

- **Número de Série**: o número de série deste dispositivo.
- **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
- **Fornecedor**: a empresa que está desenvolvendo um aplicativo de software.
- **Nome do Aplicativo**: o título de um arquivo executável. Na prática, muitos fornecedores trocam mutuamente de valores de Nomes de Aplicações e Nomes de Programas.
- **Versão**: um número que distingue lançamentos do mesmo aplicativo de software vendido separadamente, é detectado pelo agente e relatado na Central do Cliente.
- **Nome do Programa**: o título associado a um ou mais aplicativos relacionados. Na prática, muitos fornecedores trocam mutuamente de valores de Nomes de Aplicações e Nomes de Programas.

IMPORTANTE A Central do Cliente não pode mostrar informações que não consegue encontrar. Na grelha de resultados, conteúdos em branco nos campos **Fornecedor**, **Aplicativo**, **Programa** ou **Versão** indicam que os vendedores não forneceram tal informação com seus programas.

Relatório do Resumo Geral da Conformidade de Licença de Software

O Relatório da Visão Geral da Conformidade com a Licença de Software mostra o número de aplicativos licenciados ou não licenciados nos dispositivos.

Para gerar um Relatório da Visão Geral de Conformidade com a Licença de Software:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Software** > **Relatório da Visão Geral de Conformidade com a Licença de Software**.
3. Na página Relatório do Resumo Geral de Conformidade com a Licença de Software, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.

     Selecione uma das seguintes opções:
     - **Mostrar Licenças específicas da Versão** retorna um relatório que mostra o nome da licença, bem como o número da versão.
     - **Mostrar Licenças Independentes da Versão** retorna um relatório que mostra apenas o nome da licença.
   - Para filtrar seus resultados por fornecedor de software, na área **e o Fornecedor**:
     i) Digite todo ou parte do nome do fornecedor.
     ii) Clique em **Escolher** para abrir a lista e selecionar o fornecedor apropriado.
   - Para filtrar seus resultados por licença de software, na área **e o Nome da Licença contém**:
     i) Digite todo ou parte do nome do fornecedor ou clique em **Escolher** para abrir a lista e selecionar o dispositivo apropriado.
     ii) Selecione uma das seguintes opções:
       - **Exibir todas as licenças**

- **Exibir apenas as licenças que foram adquiridas ou instaladas**
   - **Exibir apenas as licenças instaladas nos Dispositivos com Agentes**

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem:
   - **Fornecedor**: uma empresa ou organização que vende aplicativos que é detectada pelo agente e relatada na Central do Cliente.
   - **Nome da Licença**: o identificador conhecido de um aplicativo instalado. Clique em um nome de licença para abrir a página Editar licença. Para mais informações, consulte "Editando Informações de Licença" na página 177.
   - **Adquisições**: O número de licenças detidas para um aplicativo.
   - **Instalado em Dispositivos sem Agente**: o número de instalações de um aplicativo em dispositivos que não têm o agente instalado.
   - **Instalado Neste Grupo**: o número de instalação de licenças de um aplicativo em um grupo. Clique em um valor para abrir o relatório de Dispositivos por Licença. Para mais informações, consulte "Relatório de Dispositivos por Licença" na página 178.
   - **Instalado em Outros Grupos**: o número de licenças de aplicativos que estão instaladas em dispositivos em um grupo de dispositivos que não estão incluídas neste relatório.
   - **Violações Disponíveis**: o número de licenças de aplicativos a serem instaladas em dispositivos. Um valor negativo nesta coluna indica que sua empresa excedeu seu número de licenças adquiridas.

IMPORTANTE A Central do Cliente não pode mostrar informações que não consegue encontrar. Na grelha de resultados, conteúdos em branco nos campos **Fornecedor**, **Aplicativo**, **Programa** ou **Versão** indicam que os vendedores não forneceram tal informação com seus programas.

Editando Informações de Licença

A pagina Editar Licença mostra o número de licenças mapeadas à Central do Cliente que foram adquiridas, instaladas e estão disponíveis para sua empresa. Você pode acessar a página Editar Licenças ao gerar o Relatório da Visão Geral de Conformidade com a Licença de Software. Consulte "Relatório do Resumo Geral da Conformidade de Licença de Software" na página 176.

Para editar as informações de licenciamento para uma licença específica:

1. Gere o relatório da visão geral de conformidade com a licença de software ao completar esta tarefa, "Relatório do Resumo Geral da Conformidade de Licença de Software" na página 176.
2. Na grelha de resultados, na coluna de **Nome de Licença**, clique no nome da licença que você deseja atualizar.
3. No campo **Licenças Adquiridas**, edite o número de licenças compradas por sua empresa.
4. No campo **Licenças Instaladas em dispositivos sem Agentes**, edite o número de dispositivos em que a licença de software foi instalada.
5. Salve suas edições ao fazer uma das seguintes ações:
   - Clique em **Salvar** para salvar suas alterações e atualizar a página Editar Licença com os novos valores.

- Clique em **Salvar e fechar** para salvar suas alterações e voltar ao Relatório da Visão Geral de Conformidade com a Licença de Software.

Relatório de Dispositivos por Licença

O Relatório de Dispositivos por Licença fornece uma lista de todos os dispositivos nos quais um aplicativo específico está instalado. Este relatório só pode ser acessado através de um link no relatório da Visão Geral da Conformidade com a Licença de Software.

Para exibir o Relatório de Dispositivos por Licença:

1. Gere um relatório da visão geral de conformidade com a licença de software. Consulte "Relatório do Resumo Geral da Conformidade de Licença de Software" na página 176.
2. Na grelha de resultados, clique em um valor na coluna **Instalado neste grupo** .
3. Na página Relatório de Dispositivos por Licença, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.

     Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.
   - Para filtrar seus resultados por um Departamento, no campo **e o Departamento é** abra a lista e selecione o departamento apropriado.
4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem:
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Número de Série**: o número de série deste dispositivo.
   - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
   - **ID de Produto**: um identificador único para um aplicativo.
   - **Sistema Operacional**: software que controla a execução de programas de computador e que pode prestar vários serviços.

Relatório do Resumo de Auditoria da Microsoft

O Relatório do Resumo de Auditoria da Microsoft é um arquivo CSV (Comma Separated Value) ou XML (eXtensible Markup Language) descarregado que relaciona todas as licenças da Microsoft exibidas no Relatório Visão Geral de Licenças de Software. Use o arquivo Resumo de Auditoria da Microsoft para rastrear a conformidade de sua empresa com os requisitos de licenciamento da Microsoft. Este arquivo atende ao layout e ao conteúdo de um dos modelos de Resumo de Auditoria da Microsoft publicados pela Microsoft.

Para gerar um Relatório do Resumo de Auditoria da Microsoft:

1. Conecte-se à Central do Cliente.
2. Faça uma das seguintes opções:
   - No painel de navegação, clique em **Relatórios** > **Ativos de Software** > **Relatório do Resumo de Auditoria da Microsoft**.
   - Na página Relatório do Resumo Geral da Conformidade de Licença de Software, clique em **Baixar resumo de auditoria da Microsoft**.
3. Na página Relatório do Resumo de Auditoria da Microsoft, no local **Nome e Formato**, no campo **Nome** insira um nome único para o relatório.
4. No campo **Formato**, abra a lista e selecione uma das seguintes opções:
   - **CSV**: um arquivo de texto simples com colunas separadas por vírgula que é aberto com software incluído no seu sistema operacional. Recomendado para consultas SQL e o carregamento de arquivos de dados grandes.
   - **XML:** um arquivo de linguagem que é aberta com um editor de XML, tal como o Microsoft Excel ou OpenOffice. Recomendado para a filtragem e a formatação de dados.
5. No local **Criar Alerta de E-mail**, no campo **Seu Endereço de E-mail**, digite seu endereço de e-mail se você deseja receber uma notificação por e-mail quando o relatório estiver processado.
6. Clique no botão **Continuar** para colocar o download em fila.

   Quando sua solicitação for processada, você pode obter o arquivo CSV ou XML do relatório na página **Meus Relatórios**. Para mais informações, consulte "Baixando Relatórios" na página 150.

   O Relatório do Resumo de Auditoria da Microsoft inclui informações de licença nos seguintes campos:

   - **Nome**: o nome da licença.
   - **Nº. de Instalações:** o número total de instâncias detectadas do aplicativo e o valor digitado manualmente para quaisquer instâncias do aplicativo instalado em dispositivos não equipados com o agente.
   - **Nº. de Licenças**: o número de licenças compradas.
   - **Nº. Disponível**: o número de licenças disponíveis para o aplicativo (números negativos indicam não-conformidade).

IMPORTANTE A Central do Cliente não pode mostrar informações que não consegue encontrar. Na grelha de resultados, conteúdos em branco nos campos **Fornecedor**, **Aplicativo**, **Programa** ou **Versão** indicam que os vendedores não forneceram tal informação com seus programas.

Relatório da Não Conformidade com a Política de Software

O Relatório de Não-Conformidade com Política de Software lista todos os dispositivos com software instalado que viola uma política de software definida, quer que a violação seja a presença de um programa de software banido ou a falta de um programa de software obrigatório. É possível também configurar o relatório para mostrar todos os dispositivos com software que, apesar de não ser banido, não está na lista de aprovados.

IMPORTANTE Para usar o Relatório de Não-Conformidade com Política de Software, primeiro você deve definir e aplicar uma política de software. Para informações sobre como definir e aplicar uma política de software, consulte "Política de Software" na página 91.

Para gerar um Relatório de Não-Conformidade com Política de Software:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Software** > **Relatório de Não Conformidade com a Política de Software**.
3. Na página Relatório da Não Conformidade com a Política de Software, na área de **Critérios de Pesquisa**, defina as opções preferidas de filtragem e de visualização para o relatório usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento é**, abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados por política, na área **e o campo**:
     i) Abra a lista e selecione um dos seguintes valores:
        - **Nome de Política**: o nome de uma Política de Software definida. Consulte "Política de Software" na página 91.
        - **Identificador**: um número de série eletrônico único atribuído ao agente instalado em um dispositivo.
        - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
        - **Fornecedor**: a empresa que está desenvolvendo um aplicativo de software.

       Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo ao usar o campo **é ou contém**, clicando em **Escolher**.

     ii) Selecione uma das seguintes opções:
        - **Possui Software na Lista de Proibidos**
        - **Software em falta na lista de obrigatórios**
   - Para filtrar seus resultados pela data, na área **e o Dispositivo chamou entre**, faça uma das seguintes ações:
     - No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados.
     - No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.

- Para retornar um relatório que mostra software que não possui uma licença definida na Central do Cliente, selecione a caixa de seleção **Mostrar software/executáveis sem licença**.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.

   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **ID da Política de Software**: o identificador único atribuído a uma Política de Software na Central do Cliente. Consulte "Política de Software" na página 91.
   - **Fornecedor**: a empresa que está desenvolvendo um aplicativo de software.
   - **Nome da Licença**: o identificador conhecido de um aplicativo instalado.
   - **Nome de Política**: o nome de uma Política de Software definida. Consulte "Política de Software" na página 91.
   - **Data da Última Chamada Rastreada**: quando o agente instalado em um dispositivo mais recentemente contactou o Centro de Monitoramento.
   - **Status**: indica se um software detectado foi banido ou está em falta.

   IMPORTANTE A Central do Cliente não pode mostrar informações que não consegue encontrar. Na grelha de resultados, conteúdos em branco nos campos **Fornecedor**, **Aplicativo**, **Programa** ou **Versão** indicam que os vendedores não forneceram tal informação com seus programas.

Relatório de Programas Instalados por Dispositivo

O Relatório de Programas Instalados por Dispositivo fornece uma lista de todos os programas de software do Windows corretamente instalados para cada dispositivo gerenciado no Grupo de Dispositivos que você especificou.

Para gerarum Relatório de Programas Instalados por Dispositivo:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Software** > **Relatório de Programas Instalados Por Dispositivo**.
3. Na página Relatório de Programas Instalados por Dispositivo, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:

   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores.
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.

- ○ **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
  - ○ **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.

  Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.

- Para filtrar seus resultados por Departamento, no campo **e o Departamento**, abra a lista e selecione o departamento desejado.
- Para filtrar seus resultados por software, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
  - ○ **Identificador de Qualquer Programa**: filtra resultados por um nome de programa, fornecedor ou versão.
  - ○ **Nome**: o título associado a um ou mais aplicativos relacionados.
  - ○ **Fornecedor**: a empresa que está desenvolvendo um aplicativo de software.
  - ○ **Versão**: um número que distingue lançamentos do mesmo programa.

  No diálogo **Escolher**, selecione o valor apropriado para definir mais este campo.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.

   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome do Programa**: o título associado a um ou mais aplicativos relacionados.
   - **Versão**: um número que distingue lançamentos do mesmo aplicativo de software vendido separadamente, é detectado pelo agente e relatado na Central do Cliente.
   - **Fornecedor**: uma empresa ou organização que vende aplicativos que é detectada pelo agente e relatada na Central do Cliente.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Departamento**: o departamento ao qual o dispositivo pertence.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Número de Série**: o número de série deste dispositivo.
   - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
   - **Sistema Operacional**: software que controla a execução de programas de computador e que pode prestar vários serviços.

   IMPORTANTE A Central do Cliente não pode mostrar informações que não consegue encontrar. Na grelha de resultados, conteúdos em branco nos campos **Fornecedor**, **Aplicativo**, **Programa** ou **Versão** indicam que os vendedores não forneceram tal informação com seus programas.

Relatório de Programas Instalados por Conta

O relatório de Programas Instalados por Conta mostra uma lista de todo o software corretamente instalado em um ou mais dispositivos rastreados que estão associados a uma conta.

Para gerar um Relatório de Programas Instalados por Conta:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Software** > **Relatório de Programas Instalados Por Conta**.
3. Na página Relatório de Programas Instalados por Conta, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento é**, abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados por um programa, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Nome**: o título associado a um ou mais aplicativos relacionados.
     - **Fornecedor**: a empresa que está desenvolvendo um aplicativo de software.
     - **Versão**: um número que distingue lançamentos do mesmo aplicativo de software.

     Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.
   - Para filtrar seus resultados por título de coluna, na área **agrupar por**, selecione uma das seguintes opções:
     - **Nome, Fornecedor e Versão** retorna um relatório que mostra o Nome, a Versão, o Fornecedor e a Quantidade do Programa.
     - **Nome e Fornecedor** retorna um relatório que mostra apenas o Nome, o Fornecedor e a Quantidade do Programa.
4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.
   - **Nome**: o título associado a um ou mais aplicativos relacionados. Na prática, muitos fornecedores trocam mutuamente de valores de Nomes de Aplicações e Nomes de Programas.
   - **Versão**: um número que distingue lançamentos do mesmo aplicativo de software vendido separadamente, é detectado pelo agente e relatado na Central do Cliente.
   - **Fornecedor**: uma empresa ou organização que vende aplicativos que é detectada pelo agente e relatada na Central do Cliente.
   - **Quantidade**: o número de aplicativos instalados em dispositivos em sua conta. Clique no valor para abrir a página do relatório de Programas Instalados Por Dispositivo – Detalhes.

IMPORTANTE A Central do Cliente não pode mostrar informações que não consegue encontrar. Na grelha de resultados, conteúdos em branco nos campos **Fornecedor**, **Aplicativo**, **Programa** ou **Versão** indicam que os vendedores não forneceram tal informação com seus programas.

Relatório de Programas Instalados por Dispositivo - Detalhes

Com o Relatório de Programas Instalados por Conta aberto, clicando em um link de valor na coluna **Quantidade** na grelha de resultados abre a página Relatório de Programas Instalados por Dispositivo – Detalhes. Esta página mostra dados com os mesmos **Critérios de Pesquisa** que você usou para o Relatório dos Programas Instalados por Conta, mas apenas para o programa específico.

A página do Relatório de Programas Instalados por Dispositivo - Detalhes fornece as seguintes informações para o programa selecionado:

- Na área de **Detalhes do Programa Instalado**:
  - **Nome**: o título associado a um ou mais aplicativos relacionados. Na prática, muitos fornecedores trocam mutuamente de valores de Nomes de Aplicações e Nomes de Programas.
  - **Fornecedor**: uma empresa ou organização que vende aplicativos que é detectada pelo agente e relatada na Central do Cliente.
  - **Versão**: um número que distingue lançamentos do mesmo aplicativo de software vendido separadamente, é detectado pelo agente e relatado na Central do Cliente.
- Na grelha de resultados:
  - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
  - **Nome**: o título associado a um ou mais aplicativos relacionados.
  - **Versão**: um número que distingue lançamentos do mesmo aplicativo de software vendido separadamente, é detectado pelo agente e relatado na Central do Cliente.
  - **Fornecedor**: uma empresa ou organização que vende aplicativos que é detectada pelo agente e relatada na Central do Cliente.
  - **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
  - **Departamento**: o departamento ao qual o dispositivo pertence.
  - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
  - **Número de Série**: o número de série deste dispositivo.
  - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
  - **Sistema Operacional**: software que controla a execução de programas de computador e que pode prestar vários serviços.

Relatórios de Segurança

Os relatórios que aparecem na página Relatórios de Segurança são determinados pelo nível de serviço que você adquiriu e podem incluir o seguinte.

- Relatório das Atualizações do Sistema Operacional
- Relatório de Configuração de Navegação na Internet
- Relatório de Software Não Autorizado
- Relatório do Antimalware
- Relatório de AntiMalware em Falta

- Relatório da Adição de Modem
- Relatório de Dispositivos Suspeitos
- Relatório de falhas de autenticação do Absolute Secure Drive
- Relatório do Status de Criptografia de Discos Completos

Relatório das Atualizações do Sistema Operacional

O relatório de Atualizações do Sistema Operacional mostra o sistema operacional instalado para cada dispositivo gerenciado.

Para dispositivos que estão executando o sistema operacional Windows, o relatório mostra detalhes sobre cada service pack e hotfix instalado no dispositivo. É também possível filtrar o relatório para mostrar dispositivos que incluem, ou que estão faltando, um hotfix específico.

Para gerar um Relatório das Atualizações do Sistema Operacional:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatórios** > **Segurança** > **Relatório das Atualizações do Sistema Operacional**.
3. Na página Relatório de Atualizações do Sistema Operacional, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento é**, abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados por sistema operacional, no campo **e o Sistema Operacional é ou contém** , insira o nome do sistema operacional.
4. Para gerar um relatório com base no nível de service packs e hotfixes dos seus dispositivos do Windows, faça o seguinte:
   a) Para filtrar seus resultados por service pack, no campo **e o service pack instalado mais recente é ou contém**, insira o nome do service pack.
   b) Para filtrar seus resultados por hotfix, na área **e os dispositivos de exibição**:
      i) Abra a lista e selecione uma das seguintes opções:
         - **com hotfix** retorna um relatório que mostra apenas dispositivos onde um hotfix foi instalado.
         - **sem o hotfix** retorna um relatório que mostra apenas dispositivos onde um hotfix não foi instalado.

      ii) No campo **hotfix é ou contém**, digite todo ou parte do nome de arquivo do hotfix.
   c) Para incluir um service pack e informações de hotfix no relatório, marque a caixa de seleção **Incluir detalhes do hotfix**.
5. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.

- **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
- **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
- **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
- **Sistema Operacional**: a versão instalado do software que controla a execução de programas de computador e que pode prestar vários serviços.
- **Service Pack**: o nível de service pack do dispositivo (aplica-se apenas a dispositivos executando o sistema operacional Windows).

  NOTA Esta coluna aparece apenas se a caixa de seleção **Incluir detalhes do hotfix** estiver marcada.

- **Hotfix do Windows**: fornece um link para o artigo da Base de Dados de Conhecimento Microsoft que descreve as alterações de software incluídas no hotfix (aplica-se a dispositivos executando somente o sistema operacional Windows).

Relatório de Configuração de Navegação na Internet

O relatório de Configurações de Navegação da Internet identifica o tipo e a versão do navegador em um dispositivo, assim como configurações de resolução de monitores de todos os dispositivos monitorados. É possível usar o relatório para identificar dispositivos que usam uma versão mais antiga de um navegador.

Para gerar um Relatório de Configuração de Navegação da Internet:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatórios** > **Segurança** > **Relatório da Configuração de Navegação na Internet**.
3. Na página Relatório da Configuração de Navegação na Internet, na área **Critérios de Pesquisa**, defina as opções de filtragem e da visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.

     Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo ao usar o campo **é ou contém**, clicando em **Escolher**.
   - Para filtrar seus resultados por Navegador, no campo **e o Nome do Navegador é ou contém**, digite todo ou parte do nome do navegador.

- Para filtrar seus resultados por versão de navegador, no campo **e a versão do navegador é ou contém**, insira a versão do navegador.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Nome do Navegador**: o nome do programa usado para acessar a internet e ver páginas web em um dispositivo.
   - **Versão do Navegador**: um número que distingue versões do navegador de internet, como detectado pelo agente e relatado na Central do Cliente.
   - **Resolução do monitor de vídeo**: o número de pixels que podem ser exibidos em um monitor de dispositivo, citado como largura x altura com as unidades em pixels, tal como 1024 x 768.
   - **Intensidade de cor**: o número de cores distintas que podem ser representadas por um determinado hardware ou software.

Relatório de Software Não Autorizado

O Relatório de Software Não Autorizado permite aos usuários pesquisar dispositivos que contêm aplicativos de software não autorizados.

Para gerar um Relatório de Software Não Autorizado:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatórios** > **Segurança** > **Relatório de Software Não Autorizado**.
3. Na página Relatório de Software Não Autorizado, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento**, abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados por um Programa, na área **e o campo**, abra a lista e selecione um dos seguintes valores.
     - **Fornecedor**: a empresa que está desenvolvendo um aplicativo de software.
     - **Programa**: um arquivo executável em um dispositivo que é detectado pelo agente e relatado na Central do Cliente.
     - **Aplicativo**: a menor unidade de software instalado em um dispositivo que é detectado pelo agente e relatado na Central do Cliente.
     - **Versão**: um número que distingue lançamentos do mesmo aplicativo de software.

- Para filtrar resultados por uma palavra-chave, no campo **que contém qualquer uma das palavras**, insira as palavras-chave.
- Para filtrar resultados por uma palavra-chave específica, no campo **contém todas as palavras**, insira palavras-chave especificas.
- Para filtrar resultados por uma frase específica, no campo **e contém exatamente a frase**, digite a frase exata.
- Para filtrar resultados excluindo palavras-chave, no campo **que não contenha qualquer uma das palavras**, insira as palavras-chave.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.

- **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
- **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
- **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
- **Departamento:** o departamento a que pertence este dispositivo.
- **Fornecedor**: a empresa que está desenvolvendo um aplicativo de software.
- **Nome do Aplicativo**: o título de um arquivo executável. Na prática, muitos fornecedores trocam mutuamente de valores de Nomes de Aplicações e Nomes de Programas.
- **Nome do Programa**: o nome de um arquivo executável em um dispositivo que é detectado pelo agente e relatado na Central do Cliente.
- **Versão**: um nome ou número único atribuído a um conjunto identificado e documentado de software.
- **Detectado pela primeira vez na Data**: a data e a hora identificada pelo agente durante a chamada para o Centro de Monitoramento.

Relatório do Antimalware

O Relatório AntiMalware identifica os dispositivos com o software antimalware instalado. É possível usar o relatório para identificar os dispositivos que estão usando uma versão antiga do software ou cujos arquivos de definição de vírus estejam desatualizados.

NOTA Para uma lista de programas antimalware e fornecedores que o agente detecta e mostra na Central do Cliente, consulte "Fornecedores de Antimalware Detectados" na página 189.

Para gerar um Relatório de Antimalware:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatórios** > **Segurança** > **Relatório de Antimalware**.
3. Na página Relatórios de Antimalware, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:

- Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.

- Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
  - **Identificador**: um número de série eletrônico único atribuído ao agente instalado em um dispositivo.
  - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
  - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.

  Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo ao usar o campo **é ou contém**, clicando em **Escolher**.
- Para filtrar seus resultados por Departamento, no campo **e o Departamento**, abra a lista e selecione o departamento desejado.
- Para filtrar seus resultados por Versão, no campo **e a versão do aplicativo AntiMalware é menor do que**, digite o valor desejado.
- Para filtrar seus resultados por Vendedor, no campo **e o Vendedor do Aplicativo é ou contém** , insira o nome do vendedor.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Departamento:** o departamento a que pertence este dispositivo.
   - **Software Antimalware**: o nome do aplicativo antimalware.
   - **Versão**: um nome ou número único atribuído a um conjunto identificado e documentado de software.
   - **Data de Definição (Texto)**: a data e a hora da definição de vírus.
   - **Definição**: a cadeia de caracteres de pesquisa usada por software antimalware para detectar um vírus de computador.
   - **Data Detectada**: a data e a hora identificada pelo agente durante a chamada para o Centro de Monitoramento.

Relatório de AntiMalware em Falta

O Relatório de Antimalware em Falta identifica todos os dispositivos monitorados que não possuem um produto de antimalware instalado.

NOTA O agente só detecta os programas antimalware e fornecedores listados no tópico, Fornecedores de Antimalware Detectados. Se o dispositivo de destino contiver um programa antimalware que não figura na lista, o agente pode não detectar com precisão a presença ou ausência do programa.

Fornecedores de Antimalware Detectados

O agente detecta e relata aplicações de antimalware e fornecedores com base em uma abordagem de dois níveis:

- **Aplicativos de Camada 1**: Aplicativos antimalware que contêm os recursos básicos de segurança que todos os dispositivos deveriam ter instalados. O agente detecta e relata aplicativos de Camada 1 que são instalados, testados e proativamente corrigidos pela Absolute Software. Consulte "Aplicativos de Camada 1" na página 190.
- **Aplicativos de Camada 2**: Aplicativos antimalware recomendados pelo vendedor para suplementar os recursos de segurança em aplicativos de antimalware de Camada 1. O agente detecta e relata aplicativos de Camada 2 que são reativamente revistos pelos clientes e corrigidos pela Absolute Software. Consulte "Aplicativos de Camada 2" na página 191.

Aplicativos de Camada 1

- Faronics Anti-Virus Engine versões 4 e 6
- Kaspersky Antivírus versões 6.0.3, 6.0.4, e 15.0.1
- Kaspersky Endpoint Security versões 8 e 10
- Kaspersky Internet Security versões 7, 14 e 15
- LANDesk Antivirus client versões 9 e 10
- Lightspeed Systems Security Agent versões 6 a 8
- McAfee VirusScan (Windows) versões 7 a 9
- McAfee Anti-Virus e Anti-Spyware (Windows) versões 15 e 16
- McAfee Security (Windows) versões 5 e 6
- McAfee Endpoint Security (Windows) versão 10
- McAfee All Access (Mac) versão 1
- McAfee Internet Security (Mac) Versão 1
- McAfee Security (Mac) Versão 1
- McAfee Endpoint Protection para Mac versão 2
- Microsoft Forefront Client Security versão 1
- Microsoft Forefront Endpoint Protection versões 2 a 4
- Microsoft Security Essentials versões 1 a 4
- Microsoft System Center 2012 Endpoint Protection versões 2 e 4
- Norton Internet Security versão 21
- Norton 360 versão 21
- Norton AntiVirus versões 11 e 12
- Symantec Antivirus versões 10.1 e 10.2
- Symantec Endpoint Protection versões 11 e 12
- Panda Internet Security 2010 versões 3, 11, e 15
- Panda Antivirus Pro 2013 versões 12 e 13
- Panda Antivirus Pro 2015
- Panda Antivirus Pro versão 13
- Panda Cloud versões 2 e 4
- Panda Endpoint versão 6
- Panda Internet Segurança 2013 versão 13
- Panda Internet Security versão 13
- Sophos Anti-Virus (Windows) versões 7 a 10
- Sophos Anti-Virus (Mac) versões 7 a 9
- Trend Micro OfficeScan Antivirus versões 8, 10 a 12
- Trend Micro Titanium (Internet Security) versão 6
- Trend Micro Internet Security versão 17
- Trend Micro Client-Server Security Agent Antivirus versão 7
- Vexira Antivirus versões 6 e 7
- Webroot SecureAnywhere versão 8

Aplicativos de Camada 2

- AhnLab V3 Internet Security versão 8
- avast! Antivirus versões 7 a 9
- AVG Anti-Virus versões 12 a 15
- AVG Anti-Virus (Business Edition) versões 13 e 14
- AVG Anti-Virus Gratuito versões gratuitas 14 e 15
- AVG CloudCare versões 14 e 15
- AVG Internet Security versões 14 e 15
- AVG AntiVirus (Mac) Versão 1
- Avira Desktop versões 12 a 14
- AntiVir Desktop versões 9 e 10
- Baidu Antivirus versões 4 e 5
- Bitdefender Antivirus versões 12 a 17
- Bitdefender Antivirus para Mac versões 2 e 3
- BullGuard AntiVirus versões 14 e 15
- CA Anti-Virus versão 6
- CA eTrust ITM versão 8
- Check Point Endpoint Security versões 7 e 8
- COMODO Antivirus versão 7
- eScan Internet Security versão 9
- ESET NOD32 Antivirus versões 5 a 7
- ESET Smart Security versões 4 a 7
- ESET Endpoint Security versão 5
- F-Prot Antivirus para Windows versões 1 e 6
- F-Secure Internet Security versão 9
- F-Secure Client Security versões 7 a 9
- FortiClient AntiVirus versão 5
- G Data AntiVirus versões 24 e 25
- Indego VirusBarrier (Mac) versão 10
- K7 AntiVirus versões 12 e 14
- Microsoft Intune versão 4
- Norman Security Suite versão 8
- Norman Virus versão 5
- Thirtyseven4 AntiVirus versão 8
- TrustPort Antivirus versão 14
- VIPRE versões 4 a 7
- ZoneAlarm Antivirus versões 12 e 13

Para gerar um Relatório de Antimalware em Falta:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatórios** > **Segurança** > Relatório de Antimalware **em falta**.
3. Na página Relatórios de Antimalware em Falta, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento**, abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Identificador**: um número de série eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.

   Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem:
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Departamento:** o departamento a que pertence este dispositivo.
   - **Nome de Usuário Atribuído**: o nome de usuário inserido ou editado por um usuário na Central do Cliente.
   - **Marca**: o fabricante de um dispositivo ou outro hardware.

     NOTA Para todos os dispositivos Chrome, a marca é **Chromebook**.
   - **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
   - **Número de Série**: o número de série deste dispositivo.
   - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.

Relatório da Adição de Modem

O Relatório de Adição de Modem identifica todos os dispositivos em que um modem foi instalado ou reconfigurado durante um determinado intervalo de datas.

Para gerar um Relatório de Adição de Modem:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatórios** > **Segurança** >Relatório**de Adição de Modem**.
3. Na página Relatório de Adição de Modem, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento**, abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Identificador**: um número de série eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.

   Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.

- Para filtrar seus resultados por data, na área **e um Modem foi instalado ou reconfigurado entre**, faça uma das seguintes ações:
  - No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados.
  - No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Data Detectada**: a data e a hora identificada pelo agente durante a chamada para o Centro de Monitoramento.
   - **Nome do Modelo Atual**: o tipo de produto de um dispositivo ou outro hardware detectado pelo agente.
   - **Porta Atual**: a porta sob qual o modem opera, como detectado pelo agente.
   - **Nome do Modelo Anterior**: o tipo de produto de um dispositivo ou outro hardware detectado anteriormente pelo agente.
   - **Porta Anterior**: a porta sob qual o modem opera, como detectado anteriormente pelo agente.

Relatório de Dispositivos Suspeitos

O Relatório de Dispositivos Suspeitos identifica todos os dispositivos que provocaram uma ou mais notificações de alerta, definidos como representativos de atividades suspeitas É possível usar a área de Alertas na Central do Cliente para especificar eventos que provocam notificações de alerta suspeitas. Para mais informações sobre a criação e gerenciamento de alertas na Central do Cliente, consulte "Alertas" na página 38.

Cenários

Por exemplo, se um grupo de dispositivos não deverá ser removido da rede em sua empresa, você pode usar o alerta de Alteração de Endereço de IP Público para registrar qualquer ocorrência quando um dispositivo no grupo for atribuído um endereço de IP diferente para acessar à Internet.

Outro exemplo é usar o alerta de Alterações Drásticas para notificar os Administradores imediatamente quando um dispositivo for detectado como tendo o **Nome do Dispositivo**, **Nome de Usuário** e a **chave do produto do Sistema Operacional** alterados simultaneamente, com o agente realizando uma chamada de auto-reparação posteriormente.

Para gerar um Relatório de Dispositivos Suspeitos:

1. Entre na Central do Cliente como um Administrador de Segurança.

2. No painel de navegação, clique em **Relatórios** > **Segurança** > Relatório **de Dispositivos Suspeitos**.
3. No Relatório de Dispositivos Suspeitos, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento**, abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Nome de Dispositivo**: o nome dado a um dispositivo.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.

     Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.
   - Para filtrar seus resultados pela data, na área **e o evento suspeito ocorreu**, faça uma das seguintes ações:
     - No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados.
     - No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.
   - Para filtrar seus resultados por nível de suspeita, na área**e o nível de suspeita é**:
     i) Abra a lista e selecione um valor para **Maior que**, **Igual a**, ou **Menor que**.
     ii) Abra a lista e selecione o **Nível de Suspeita** desejado.
4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Nome de Dispositivo**: o nome dado a um dispositivo.
   - **Marca**: o fabricante de um dispositivo ou outro hardware.
   - **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
   - **Nível de suspeita**: o nível de severidade de um evento suspeito. Possíveis valores variam desde **Não é Suspeito** até um nível de suspeição de**5**.

- **Eventos Suspeitos**: clique o valor para abrir a página Eventos de Alerta para ver o nome do alerta e a descrição.

Relatório de falhas de autenticação do Absolute Secure Drive

O relatório de falhas de autenticação do Absolute Secure Drive mostra uma lista daqueles dispositivos que o Absolute Secure Drive falhou em autenticar com base nas opções que você definiu.

É possível filtrar este relatório com base na frequência das falhas na autenticação, tipos de autenticação ou tipos de falhas disponíveis.

É também possível definir um altera para notifica-lo sobre tentativas de login no Absolute Secure Drive ao selecionar a condição **Falha de login no Absolute Secure Drive** na página Criar e Editar Alertas. Para mais informações, consulte "Criando Novos Alertas Personalizados" na página 43.

Para gerar um Relatório de falhas de autenticação do Absolute Secure Drive:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Segurança** > Relatório **do Absolute Secure Drive**.
3. Na página Relatórios de Falhas de Autenticação do Absolute Secure Drive, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Nome de Dispositivo**: o nome dado a um dispositivo.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.

     Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.
   - Para filtrar seus resultados pela data, na área **e quando ocorreram tentativas de autenticação falhadas**, faça uma das seguintes ações:
     - No campo **ou mais vezes**, digite o número apropriado de tentativas de login falhadas que deseja ver no seu relatório.
     - Selecione uma das seguintes opções:
       – No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados.
       – No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.
   - Para filtrar seus resultados por tipo de falha de autenticação, na área **e o tipo de falha é**:

i) Abra a lista **Tipos de Autenticação** e selecione um dos seguintes valores:
   - **Todos os Tipos de Autenticação** onde a componente de autenticação é um ou mais dos seguintes valores.
   - **Senha Mestre** onde a senha digitada é autenticada usando a senha atual como referência.
   - **Impressão Digital** onde o input de um scanner de impressão digital é autenticado usando o valor atual como referência.
   - **RFID** onde o input de um dispositivo RFID é autenticado usando o valor atual como referência.
   - **SmartCard** onde o input de um chip ou cartão de circuito integrado (ICC) é autenticado usando o valor atual.

ii) Abra a lista **Tipos de Falhas** e selecione um dos seguintes valores:
   - **Todos os Tipos de Falhas** onde a falha é um ou mais dos seguintes valores.
   - **Autenticação Falhou** onde a senha ou a autenticação de login não correspondeu ao valor atual.
   - **Falha de Componente** onde a componente de autenticação, tal como RFID ou dispositivo de reconhecimento de impressões digitais, falhou.
   - **Usuário Desconhecido** onde o nome de usuário é desconhecido ou não corresponde o valor atual.
   - **Demasiadas Tentativas** onde o nome de usuário ou componente deste tentou se conectar mais do que um número específico de vezes com credenciais incorretas.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome de Dispositivo**: o nome dado a um dispositivo.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Número de logins falhados:** o número de falhas na autenticação nas tentativas de login do Absolute Secure Drive.
   - **Hora da Chamada**: quando o dispositivo contatou o Centro de Monitoramento.
   - **Data Registrada (UTC)**: a data e a hora quando as falhas de autenticação foram registradas.
   - **Nome de Usuário Experimentado**: o nome de usuário que foi usado quando a falha de autenticação ocorreu.
   - **Tipo de login falhado**: o tipo de falha de autenticação, que é uma mistura dos campos **Tipo de Autenticação** e **Tipo de Falha** , por exemplo, **Senha Mestra: Falhou** ou **Senha Mestra: Usuário Desconhecido**.
   - **Status de Criptografia**: o status de criptografia disponível no dispositivo. Clique no link **Ver Status de Criptografia** para abrir o Relatório do Status de Criptografia de Discos Completos.

Relatório do Status de Criptografia de Discos Completos

Criptografia de Disco Completo (FDE - Full-disk encryption) é uma solução de hardware ou de software que protege, ou criptografa, todo o conteúdo de uma unidade física.

O Computrace detecta hardware FDE (unidades de criptografia automática) e produtos de software de criptografia de discos completos que estão instalados nos discos rígidos dos dispositivos Windows e Mac gerenciados de sua empresa. Cada fornecedor de criptografia usa cadeias de status de criptografia específicas em seus produtos.

IMPORTANTE Atualmente, o Relatório do Status de Criptografia de Discos Completos fornece apenas informações sobre produtos de criptografia de discos completos instalados no sistema ou na primeira unidade física

Usando a filtragem disponível com o Relatório de Status de Criptografia da Central do Cliente, você pode pesquisar os dispositivos rastreados de sua conta para detectar aqueles dispositivos que têm a criptografia ativa e retornar os resultados mostrados com base em seu filtro no Relatório do Status de Criptografia de Discos Completos - Produtos Detectados É possível salvar os filtros usados para criar versões específicas do Relatório do Status de Criptografia de Discos Completos - Produtos Detectados para seu local de **Meus Filtros** na Central do Cliente.

É possível também criar um relatório daqueles dispositivos rastreados que não têm a criptografia por hardware ou por software ativada. O Relatório do Status de Criptografia de Discos Completos - Produtos Não Detectados inclui uma coluna intitulada **Habilitado com SED** que indica se um dispositivo tem uma unidade de auto-criptografia (SED) com possibilidades de FDE, mas que pode não estar ativado ou suportado pelo Computrace. Esta funcionalidade fornece a você a oportunidade de remediar essa situação.

A partir do Relatório do Status de Criptografia de Discos Completos, você pode criar alertas para notificar de quando as condições que você forneceu nos detalhes de filtragem são atendidas. Criando um alerta a partir deste relatório preencherá as condições na página Criar e Editar Alertas com aquelas mostradas no relatório. Para mais informações sobre a criação deste tipo de Alertas, consulte "Criando um Alerta Baseado em Critérios de Status de Criptografia de Discos Completos" na página 46.

Esta seção fornece informações sobre os seguintes tópicos e tarefas:

- Produtos de software de criptografia de discos completos e unidades de auto-criptografia detectados
- Ligando a Recolha de Dados de Criptografia de Discos Completos para sua Conta.
- Filtrando Dados para Criar um Relatório do Status de Criptografia de Discos Completos
- Identificando Dispositivos que Tem Produtos de Criptografia Instalados
- Identificando Dispositivos Sem Produtos de Criptografia de Discos Completos Instalados
- Vendo alterações à Cadeia do Status de Criptografia de um Dispositivo
- Visualizando o Histórico da Criptografia de Discos Completos de um Dispositivo:
- Desligando a Recolha de Dados de Criptografia de Discos Completos para sua Conta.

Produtos de software de criptografia de discos completos e unidades de auto-criptografia detectados

IMPORTANTE Atualmente, o Relatório do Status de Criptografia de Discos Completos fornece somente informações sobre produtos de criptografia de discos completos instalados no sistema ou na primeira unidade física apenas.

O Computrace coleta dados de FDE dos vendedores de produtos de software de FDE e unidades de auto-criptografia e retorna os dados nos seguintes relatórios:

- Relatório do Status de Criptografia de Discos Completos - Produtos Detectados
- Relatório do Status de Criptografia de Discos Completos - Produtos Não Detectados

Produtos de FDE e unidades de auto-criptografia detectados em dispositivos do Windows

Nome do Vendedor	Nome do Produto	Versão	Tipo de Criptografia
Absolute Software Corporation	Absolute Secure Drive	7 e 8	hardware
Becrypt, Inc.	Becrypt DISK Protect	5	software
Check Point Software Technologies Ltd.	Criptografia de Disco Completo da CheckPoint	7 e 8	software
	Pointsec para PCs	6	software
Credant Technologies (adquirida pela Dell)	Criptografia de Volumes Completos Credant	6, 7 e 8	software
	Credant Mobile Guardian	5, 6, 7 e 8	software
	DataArmor	3	software
DesLock Ltd	DesLock+	4	software
GuardianEdge Technologies, Inc. (adquirida pela Symantec Corporation)	Disco Rígido GuardianEdge	8 e 9	software
Kaspersky Lab	Kaspersky Endpoint Security	10	software
McAfee, Inc.	Criptografia de Endpoint McAfee	5, 6 e 7	software
	Criptografia de Unidades McAfee	7	software
	McAfee	7	software
Microsoft Corporation	Criptografia de Unidades BitLocker	6	software
PGP Corporation (adquirida pela Symantec Corporation)	PGP	9	software
	PGP Desktop	9 e 10	software
EgoSecure	FinallySecure (anteriormente propriedade da Secude AG)	9	software

Produtos de FDE e unidades de auto-criptografia detectados em dispositivos do Windows (continuado)

Nome do Vendedor	Nome do Produto	Versão	Tipo de Criptografia
SafeBoot International	Criptografia de Dispositivos SafeGuard	4	software
SecurStar	DriveCrypt Plus Pack	1, 3, 4 e 5	software
Symantec Corporation	Criptografia de Endpoint Symantec	8	software
	Criptografia Symantec	10	software
Trend Micro	Criptografia de Discos Completos Trend Micro	3	software
TrueCrypt Foundation	TrueCrypt	6 e 7	software
Sophos	Criptografia de Dispositivos SafeGuard®	5 e 6	software
	SafeGuard Easy	4	software
Wave Systems Corp.	EMBASSY® Trusted Drive Manager	4	hardware
WinMagic Inc.	Criptografia de Discos SecureDoc	5 e 6	hardware e software

Produtos FDE detectados em dispositivos Mac

Nome do Vendedor	Nome do Produto	Versão	Tipo de Criptografia
Apple Inc.	FileVault	10	hardware
PGP Corporation (adquirida pela Symantec Corporation)	PGP	9 e 10	software
	Encryption Desktop	10	software
TrueCrypt Foundation	TrueCrypt	6 e 7	software
Sophos	Sophos SafeGuard®	5 e 6	software
WinMagic Inc.	SecureDoc	6	hardware e software

Ligando a Recolha de Dados de Criptografia de Discos Completos para sua Conta.

Por padrão, a recolha de dados de criptografia de discos completos está desligado tanto no Computrace como na Central do Cliente. É possível recolher dados de criptografia de discos completos em seus dispositivos Windows e Mac gerenciados ao ligar essa função no Relatório do Status de Criptografia de Discos Completos (se você for um usuário novo) ou usando a página Configurações de Conta. Atualmente, o Relatório do Status de Criptografia de Discos Completos fornece somente informações sobre produtos de criptografia de discos completos instalados no sistema ou na primeira unidade física apenas.

NOTA O tempo que leva para a coleção de dados de criptografia de discos completos a começar ou a parar depende da frequência com que um dispositivo faz chamadas de agente.

Para ligar a recolha de dados de criptografia de discos completos a partir do Relatório do Status de Criptografia de Discos Completos:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatórios** > **Segurança** > **Relatório do Status de Criptografia de Discos Completos**.
3. Quando usuários novos abrem o Relatório do Status de Criptografia de Discos Completos, um botão de **Começar Recolha de Dados** aparece. Clique em **Começar Recolha de Dados** para começar recolhendo dados de criptografia de discos completos a próxima vez que este dispositivo fizer uma chamada de agente.

   A página Relatório do Status de Criptografia de Discos Completos se atualiza e mostra uma mensagem de confirmação dizendo que a recolha de dados foi ativada e que a mesma poderá demorar algum tempo antes dos dados recolhidos estarem disponíveis deste relatório.

Para ligar a recolha de dados de criptografia de discos completos a partir de dispositivos usando a página Configurações de Conta:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Administração** > **Conta** > **Configurações de Conta**. A página Configurações de Contas é aberta.
3. Na página Configurações de Conta, na área **Status de Criptografia de Discos Completos**, marque a caixa de seleção de **Recolher dados de criptografia de discos completos a partir de dispositivos**.

É possível desativar a recolha de dados para produtos de criptografia de discos completos em seus dispositivos. Para mais informações, consulte "Desligando a Recolha de Dados de Criptografia de Discos Completos para sua Conta." na página 207.

Filtrando Dados para Criar um Relatório do Status de Criptografia de Discos Completos

A área de **Critérios de Pesquisa** no Relatório de Criptografia de Discos Completos fornece uma funcionalidade semelhante à maioria de outros relatórios (consulte "Gerando Relatórios" na página 138.), com várias exceções que lhe são particulares.

Para filtrar dados para criar um relatório do Status de Criptografia de Discos Completos:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatórios** > **Segurança** > **Relatório do Status de Criptografia de Discos Completos**.
3. No Relatório do Status de Criptografia de Discos Completos, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:

- Para filtrar seus resultados por produtos de criptografia de discos completos detectados ou não, no local **o produto de Criptografia de Discos Completos é** , selecione uma das seguintes opções:
  - Clique em **detectado** para retornar um relatório que mostra dispositivos onde FDE é detectado. Para mais informações, consulte "Identificando Dispositivos que Tem Produtos de Criptografia Instalados" na página 203.
  - Clique **não detectado** para retornar um relatório que mostra aqueles dispositivos em que nenhum produto de FDE é detectado. Selecionando esta opção acrescenta uma coluna de **Habilitado para SED** à grelha de resultados. Para mais informações, consulte "Identificando Dispositivos Sem Produtos de Criptografia de Discos Completos Instalados" na página 205.
- Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
- Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
  - **Quaisquer dos campos nesta lista**: seleciona todos os valores na lista.
  - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
  - **Nome de Dispositivo**: o nome dado a um dispositivo.
  - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
  - **Nome do Produto**: o nome do software de criptografia de discos completos.
  - **Versão do Agente**: o número de versão do produto (ou programa) de criptografia de discos completos detectado.
  - **Descrição de Unidade**: os dados de criptografia coletados para mostrar apenas aqueles dispositivos com os atributos detectados que correspondem a esta descrição da unidade de disco.
  - **Número de Série da Unidade**: os dados de criptografia recolhidos para dispositivos onde este número de série de unidade é detectado nos discos rígidos dos dispositivos de sua conta.

  Dependendo do valor que você selecionou da lista, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.
- Para filtrar seus resultados pela data, na área **e a última Chamada de Agente ocorreu**, faça uma das seguintes ações:
  - No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resulta em um relatório maior e demora mais tempo a gerar resultados.
  - No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.
- Para filtrar seus resultados por unidade de auto-criptografia, no campo **e o Dispositivo possui uma Unidade de Auto-Criptografia**, faça uma das seguintes ações:
  - **Qualquer**: mostra dispositivos com criptografia de software ou de hardware.
  - **Sim (Habilitado para SED)**: mostra dispositivos com uma unidade de auto-criptografia.
  - **Não**: mostra dispositivos sem uma unidade de auto-criptografia.

- ○ **Não Detectado**: mostra dispositivos que não têm uma unidade SED detectada.

- Para filtrar resultados por cadeia do status de criptografia usada por um vendedor em particular, que está criptografada em um dispositivo, na área **e onde a cadeia do Status de Criptografia**, faça o seguinte:
  i) No campo **Selecione uma regra**, abra a lista e selecione a regra desejada.
  ii) Digite as condições baseadas na **Cadeia de Status de Criptografia** de vendedores. Para mais informações, consulte "Vendo alterações à Cadeia do Status de Criptografia de um Dispositivo" na página 206.
  iii) Quando você tiver introduzido até cinco condições específicas às cadeias de status de criptografia dos Vendedores clique em **Adicionar Condição**.

  Se você introduzir mais do que cinco condições, o botão de **Adicionar Condição** torna-se inacessível até haver apenas cinco condições. As condições permitem apenas argumentos de *e*. Não é possível introduzir um argumento de *ou*.

  Se você não adicionar quaisquer condições, todos as cadeias de Status de Criptografia aparecerão no relatório.

  NOTA É possível **Criar um alerta baseado neste critério de status de criptografia** ao clicar neste link. Se você quiser salvar a informação de filtro que inseriu, precisa de salvá-la antes de criar um alerta de criptografia de discos completos. Para essas instruções e para adicionar mais condições, consulte "Criando um Alerta Baseado em Critérios de Status de Criptografia de Discos Completos" na página 46.

- Na área **O status mudou desde a última chamada de agente**, clique na caixa de seleção para ver aqueles dispositivos cujo status de criptografia mudou no tempo entre as duas últimas chamadas de agente.

  Para alertas, se houver uma alteração no status entre a última chamada e a próxima chamada de agente, o alerta é acionado.

- Se o Bitlocker for seu produto de criptografia de discos completos principal, limpe a caixa de seleção **Mostrar detecções não criptografadas do Microsoft BitLocker como não detectadas**.

  Na ausência de um produto de criptografia de discos completos, o Computrace detecta o Microsoft BitLocker na maioria de plataformas do Windows porque os drivers estão presentes mesmo que o recurso não esteja ativo.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem:

   IMPORTANTE Atualmente, o Relatório do Status de Criptografia de Discos Completos fornece somente informações sobre produtos de criptografia de discos completos instalados no sistema ou na primeira unidade física apenas.

   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome de Dispositivo**: o nome dado a um dispositivo.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Nome de produto**: o nome do programa de criptografia detectado.

- **Versão do Agente**: o número de versão do produto (ou programa) detectado de criptografia.
- **Cadeia do Status da Criptografia**: a cadeia detectada do fornecedor de criptografia, que poderá estar truncada devido ao comprimento. Abra a dica de ferramenta para ver a cadeia inteira, que você pode copiar se for necessário.
- **Algoritmo**: o algoritmo detectado e usado pelo programa de criptografia, se disponível.
- **Descrição de Unidade**: a descrição detectada do disco rígido deste dispositivo.
- **Número de Série da Unidade**: o número de série detectado da unidade de criptografia neste dispositivo.
- **Com capacidade para SED**: indica que uma unidade com capacidade para SED foi detectada neste dispositivo, no entanto, a criptografia pode não ser gerenciada por software de gerenciamento de SED.
- **Última Chamada**: a data e a hora quando a última chamada de agente foi feita neste dispositivo.
- **Última reinicialização**: a data e a hora da última vez que este dispositivo foi reiniciado.
- **Aplicativo Iniciado**: a data e a hora da última vez que o aplicativo foi iniciado.
- O link do **Histórico** abre o Relatório do Histórico da Criptografia que exibe as 10 alterações mais recentes à cadeia do status de criptografia para este dispositivo. Para mais informações, consulte "Visualizando o Histórico da Criptografia de Discos Completos de um Dispositivo:" na página 206.

Para informações sobre cada relatório, consulte os seguintes tópicos:

- "Identificando Dispositivos que Tem Produtos de Criptografia Instalados" na página 203
- "Identificando Dispositivos Sem Produtos de Criptografia de Discos Completos Instalados" na página 205

Identificando Dispositivos que Tem Produtos de Criptografia Instalados

IMPORTANTE Atualmente, o Relatório do Status de Criptografia de Discos Completos fornece apenas informações sobre produtos de criptografia de discos completos instalados no sistema ou na primeira unidade física

Para executar um relatório que mostra os dispositivos em sua conta que têm software de criptografia de discos completos instalado no disco rígido que contém o sistema operacional ou que têm uma SED:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatórios** > **Segurança** > **Relatório do Status de Criptografia de Discos Completos**.
3. No Relatório do Status de Criptografia de Discos Completos, na seção **Critérios de Pesquisa**, na área **o Produto de Criptografia de Discos Completos é**, clique na opção **detectado**.
4. Digite todos os critérios de filtragem desejados como descrito na tarefa, "Filtrando Dados para Criar um Relatório do Status de Criptografia de Discos Completos" na página 200.
5. Veja a grelha de resultados para ver o que o Computrace detectou.

   NOTA Se nada aparecer em uma coluna, então essa informação não foi fornecida pelo fornecedor e, portanto, não poderá ser detectada pelo Computrace.

- **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
- **Nome de Dispositivo**: o nome dado a um dispositivo.
- **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
- **Nome de produto**: o nome do programa de criptografia de discos completos detectado.
- **Versão do Agente**: o número de versão do produto (ou programa) detectado de criptografia.
- **Cadeia do Status da Criptografia**: a cadeia detectada do fornecedor de criptografia de discos completos, que poderá estar truncada devido ao comprimento. Abra a dica de ferramenta para ver a cadeia inteira, que você pode copiar se for necessário.

NOTA Mensagens são fornecidas sobre se a unidade está criptografada ou não, ou se há quaisquer erros.

- **Algoritmo**: o algoritmo detectado e usado pelo programa de criptografia, se disponível.
- **Descrição de Unidade**: a descrição detectada do disco rígido deste dispositivo.
- **Número de Série da Unidade**: o número de série detectado para a unidade criptografada neste dispositivo.
- **Habilitado para SED**: indica que uma unidade habilitado para SED foi detectada neste dispositivo, no entanto, a criptografia de discos completos pode não ser gerenciada por software de gerenciamento de SED.
- **Última Chamada**: a data e a hora quando a última chamada de agente foi feita neste dispositivo.
- **Última reinicialização**: a data e a hora da última vez que este dispositivo foi iniciado.
- **Aplicativo Iniciado**: a data e a hora da última vez que o aplicativo foi iniciado.
- O link do **Histórico** abre o Relatório do Histórico da Criptografia que exibe as 10 alterações mais recentes à cadeia do status de criptografia para este dispositivo. Para mais informações, consulte "Visualizando o Histórico da Criptografia de Discos Completos de um Dispositivo:" na página 206.

As informações de **Última Reinicialização** e **Início de Aplicativo** são importantes em situações de furto quando se constata que estas datas são posteriores à **Data do Furto**. Isto significa que o ladrão conseguiu se conectar no dispositivo, tendo ultrapassado a autenticação de pré-inicialização e o arranque do produto de criptografia de discos completos. Tais casos indicam que o ladrão poderá ter acesso ao dispositivo e que o furto podia ter sido um furto interno. O Relatório do Histórico de Criptografia também é útil neste tipo de situação de furto porque mostra as 10 últimas alterações ao dispositivo. Consulte "Visualizando o Histórico da Criptografia de Discos Completos de um Dispositivo:" na página 206.

Identificando Dispositivos Sem Produtos de Criptografia de Discos Completos Instalados

Executando um relatório que mostra os dispositivos em sua conta em que o Computrace não detectou nenhum produto de software de criptografia de discos completos instalado no disco rígido (contendo o Sistema Operacional) permite a você saber se existem discos rígidos onde você pode instalar um produto de criptografia de hardware. Este relatório também permite que você saiba se quaisquer SEDs foram detectados. Se sim, então talvez os SEDs não estejam a ser gerenciados por software de gerenciamento de SED. É possível também ver que tipo de disco foi detectado ao olhar para a informação na **Descrição de Unidade** e no **Número de série de Unidade**.

Para executar um relatório que mostra os dispositivos em sua conta em que o Computrace não detectou nenhum produto de software de criptografia de discos completos instalado no disco rígido:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatórios** > **Segurança** > **Relatório do Status de Criptografia de Discos Completos**.
3. No Relatório do Status de Criptografia de Discos Completos, na área **Critérios de Pesquisa**, na área **o Produto de Criptografia de Discos Completos é**, clique na opção **não detectado**.
4. Digite todos os critérios de filtragem desejados como descrito na tarefa, "Filtrando Dados para Criar um Relatório do Status de Criptografia de Discos Completos" na página 200.

   NOTA Quando você quiser mostrar dispositivos em que **a Criptografia não é detectada**, a opção de filtragem da **Cadeia do Status da Criptografia** não está disponível.

5. Veja a grelha de resultados, que mostra a seguinte informação específica àquilo que foi detectado pelo Computrace.

   NOTA Se nada aparecer em uma coluna, então essa informação não foi fornecida pelo fornecedor e, portanto, não poderá ser detectada pelo Computrace.

   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome de Dispositivo**: o nome dado a um dispositivo
   - **Nome de Usuário**: o nome único detectado pelo agente para identificar uma pessoa que está usando o dispositivo.
   - **Status** não está disponível neste modo porque não há nenhum produto de software FDE instalado.
   - **Descrição de Unidade**: a descrição detectada do disco rígido deste dispositivo.
   - **Número de Série da Unidade**: o número de série detectado da unidade de criptografia neste dispositivo.
   - **Com capacidade para SED**: indica que uma unidade com capacidade para SED foi detectada neste dispositivo, no entanto, a criptografia pode não ser gerenciada por software de gerenciamento de SED.
   - **Última Chamada**: a data e a hora quando a última chamada de agente foi feita neste dispositivo.

- O link do **Histórico** abre o Relatório do Histórico da Criptografia que mostra as 10 alterações mais recentes da cadeia do status de criptografia deste dispositivo. Para mais informações, consulte "Visualizando o Histórico da Criptografia de Discos Completos de um Dispositivo:" na página 206.

Vendo alterações à Cadeia do Status de Criptografia de um Dispositivo

Alterações nas cadeias de Status de Criptografia de um dispositivo podem indicar qualquer uma das seguintes situações:

- um usuário instalou um produto de criptografia diferente
- um disco criptografado que você não estava rastreando está agora sendo rastreado
- houve outras alterações
- um disco criptografado foi removido do dispositivo

Definindo um alerta para estas situações permite que você saiba quando elas acontecem, sem você ter que determinar estas alterações ao analisar o relatório do status de criptografia de discos completos sem auxílio. Para mais informações, consulte "Criando um Alerta Baseado em Critérios de Status de Criptografia de Discos Completos" na página 46.

Para ver alterações à cadeia do status da criptografia de um dispositivo:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatórios** > **Segurança** > **Relatório do Status de Criptografia de Discos Completos**.
3. No Relatório do Status de Criptografia de Discos Completos, na área **o Produto de Criptografia de Discos Completos é**, clique em **detectado**.
4. Na área **Critérios de Pesquisa**, digite os dados de filtragem desejados, conforme as instruções na tarefa, "Filtrando Dados para Criar um Relatório do Status de Criptografia de Discos Completos" na página 200.
5. Na área de **e onde a cadeia do Status de Criptografia**, faça o seguinte:
   a) Abra a lista e clique em **Contém** e digite `Disco de sistema`.
   b) Clique em **Adicionar Condição**.
   c) Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e mostra todos os dispositivos que contêm **disco de sistema** sob a coluna de **Cadeia do Status da Criptografia**.

Visualizando o Histórico da Criptografia de Discos Completos de um Dispositivo:

É possível ver as últimas 10 alterações à Cadeia do Status da Criptografia de Discos Completos de um dispositivo ao abrir seu Relatório do Histórico de Criptografia de Discos Completos.

Para ver o Relatório do Histórico da Criptografia de Discos Completos de um Dispositivo:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, **Relatórios** > **Segurança** > **Relatório do Status de Criptografia de Discos Completos**.

3. No Relatório do Status de Criptografia de Discos Completos, na área **Critérios de Pesquisa**, digite os dados de filtragem desejados, conforme as instruções na tarefa, "Filtrando Dados para Criar um Relatório do Status de Criptografia de Discos Completos" na página 200.
4. Clique em **Mostrar resultados** e na grelha de resultados atualizada, localize o dispositivo apropriado, role para a extrema direita da grelha e clique no link do **Histórico** desse dispositivo.
5. O Relatório do Histórico de Criptografia para o dispositivo escolhido se abre e mostra a você a seguinte informação:

   IMPORTANTE Atualmente, o Relatório do Status de Criptografia de Discos Completos fornece apenas informações sobre produtos de criptografia de discos completos instalados no sistema ou na primeira unidade física

   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome de Dispositivo**, que é o nome dado a um dispositivo.
   - **Nome de Usuário**, que é o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Nome de produto**, que é o nome do programa de criptografia de discos completos detectado.
   - **Versão**, que é o número de versão do produto (ou programa) detectado de criptografia.
   - **Tipo de Criptografia**, que indica se a criptografia de discos completos do dispositivo detectada é software ou hardware.
   - **Cadeia do Status de Criptografia**, que é detectada do fornecedor de criptografia, que poderá estar truncada devido ao cumprimento. Abra a dica de ferramenta para ver a cadeia inteira, que você pode copiar se for necessário.
   - **Algoritmo**, que é o algoritmo detectado e usado pelo programa de criptografia, se disponível.
   - **Descrição de Unidade**, que é a descrição detectada do disco rígido deste dispositivo.
   - **Número de Série da Unidade**, que é o número de série detectado da unidade de criptografia neste dispositivo.
   - **Data da Chamada**, que é a data e a hora quando a última chamada de agente foi feita neste dispositivo.
   - **Última Reinicialização**, que é a data e a hora da última vez que este dispositivo foi reiniciado.
   - **Aplicativo Iniciado**, que é a data e a hora da última vez que o aplicativo foi iniciado.
   - **Data de Ação**, que é a data e a hora quando uma entrada foi adicionada ao relatório do histórico da criptografia de discos completos deste dispositivo.
6. Clique em **<<Voltar** para voltar à página Relatório do Status de Criptografia de Discos Completos.

Desligando a Recolha de Dados de Criptografia de Discos Completos para sua Conta.

É possível desligar a recolha de dados de criptografia de discos completos da sua conta. Esta configuração se encontra na página Configurações de Conta na área **Status de Criptografia de Discos Completos**. Para mais informações, consulte "Gerenciando Configurações de Conta" na página 116.

Relatórios de Histórico de Chamadas e Controle de Perdas

Use os relatórios de Histórico de Chamadas e Controle de Perdas para assegurar que seus dispositivos chamem o Centro de Monitoramento regularmente a partir de locais esperados e indiquem usuários esperados. Se um dispositivo chamar o Centro de Monitoramento regularmente, a chance de recuperação é muito maior quando um dispositivo estiver desaparecido. Para ser elegível para o pagamento da Garantia de Serviço após um dispositivo ser furtado, o dispositivo deve fazer pelo menos uma chamada pós-furto.

As seguintes informações e relatórios são fornecidos nesta seção:

- Informação de Chamada de IP Estendido
- Relatório do Histórico de Chamadas
- Relatório de Dispositivos em Falta
- Relatório de Desvio de Dispositivos por Nome de Dispositivo
- Relatório de Desvio de Dispositivos pelo Usuário
- Relatório do Histórico de Desvio de Dispositivos
- Relatório de Ativação
- Relatórios de Rastreamento de Geolocalização

Informação de Chamada de IP Estendido

Relatórios de Histórico de Chamadas, de Dispositivos Desaparecidos e de Desvios de Dispositivos podem conter informações de identificação de quem esta ligando. As informações de quem esta ligando aparecem geralmente como um link. Clicando no link abre a página Informação de Chamada de IP Estendida, que fornece detalhes sobre o local ou a origem de um endereço de IP ou número de telefone. As informações são úteis para quando se está localizando dispositivos que estão fora da rede empresarial.

A página Informação de Chamada de IP Estendida lista as seguintes informações:

- Identificador
- Hora do Servidor
- Endereço IP Local
- Endereço IP Proxy
- Nome do Host
- Endereço MAC
- RDNS do IP local
- RDNS do IP do proxy
- Informações ARIN Who IS

Relatório do Histórico de Chamadas

O Relatório do Histórico de Chamadas mostra todas as comunicações para o Centro de Monitoramento feitas por um Identificador específico ou por um grupo de Identificadores.

IMPORTANTE Os dados de chamadas ficam armazenados online por um ano e, depois desse período de tempo, são arquivados. Se um Relatório de Histórico de Chamadas estiver configurado para exibir dados com mais de um ano, é necessário recuperar os dados do servidor de arquivamento e o relatório demora mais tempo para gerar os resultados.

Para gerar um Relatório do Histórico de Chamadas:

1. Conecte-se à Central do Cliente.

2. No painel de navegação, clique em **Relatórios** > **Histórico de Chamadas e Controle de Perdas** > **Relatório do Histórico de Chamadas**.
3. No Relatório do Histórico de Chamadas, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores.
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
     - **Nome de Usuário Atribuído**: o nome de usuário atribuído a um dispositivo por um administrador de sistemas na página Visualizar e Editar Dados de Campos Definidos pelo Usuário.
     - **Número de Série**: o número de série do dispositivo ou outro hardware.
     - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.

     Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento é**, abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados pela data, na área **e a chamada ocorreu**, faça uma das seguintes ações:
     - No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados.
     - No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.
   - Para filtrar seus resultados por um endereço de IP específico, no local **e o endereço IP para**:

     i) Abra a lista e selecione uma das seguintes opções:
       - **IP Público**
       - **IP Local**

     ii) Digite um endereço IP válido.
4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.

NOTA A cor do plano de fundo de cada cabeçalho de coluna indica a aplicabilidade da informação. Informações atuais têm uma cor mais clara enquanto informações que se aplicavam na hora da chamada do agente têm uma cor ligeiramente mais escura.

- **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
- **Número de Série**: o número de série do dispositivo ou outro hardware.
- **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
- **Marca**: o fabricante do dispositivo.

NOTA Para todos os dispositivos Chrome, a marca é **Chromebook**.

- **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
- **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
- **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
- **Hora da Chamada**: quando o dispositivo contatou o Centro de Monitoramento.

NOTA Para dispositivos Chrome, esta coluna mostra a data e a hora em que as informações de dispositivo na Central do Cliente foram sincronizadas com as informações de dispositivo na sua conta do Google.

- **Localização (Latitude e Longitude)**: a posição de um dispositivo na superfície da terra, expressada em latitude e longitude.
- **Endereço IP Local**: o endereço IP atribuído a um dispositivo na Rede Local (LAN) ao chamar o Centro de Monitoramento.
- **Endereço de IP Público**: o endereço IP usado para comunicar com a Internet. Para chamadas de modem, a Central do Cliente relata informação de identificação de chamadas. Clique no link de **Endereço de IP Público** para abrir a página Informações de Chamadas de IP Estendidas. Consulte "Informação de Chamada de IP Estendido" na página 208.

Relatório de Dispositivos em Falta

O relatório de Dispositivos em Falta lhe permite identificar os dispositivos que não contataram o Centro de Monitoramento dentro do período de tempo designado.

Revise periodicamente os Identificadores atribuídos aos dispositivos na sua empresa. Verifique se há algum dispositivo que não entrou em contato com o Centro de Monitoramento por um período de tempo longo e fora do normal (ex.: 45 dias). A falta de contato de um dispositivo pode indicar que o agente está em falta ou que um evento ocorreu que está impedindo o agente de entrar em contato com o Centro de Monitoramento. Dispositivos dormentes estão automaticamente excluídos do relatório . Pode ser necessário ajustar o valor do **filtro de Chamadas Mais Recentes** para que a grelha de resultados contenha resultados. Consulte "Informação de Chamada de IP Estendido" na página 208.

Para gerar um Relatório de Dispositivos em Falta:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Histórico de Chamadas e Controle de Perdas** > **Relatório de Dispositivos em Falta**.

3. No Relatório de Dispositivos em Falta, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento é**, abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados por chamadas de agente, no campo **e a Chamada mais recente é de há mais de**, insira um valor para o número de dias.
4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Número de Série**: o número de série do dispositivo ou outro hardware.
   - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
   - **Marca**: o fabricante do dispositivo.

     NOTA Para todos os dispositivos Chrome, a marca é **Chromebook**.
   - **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
   - O link para o **Histórico de Chamadas** abre o Relatório do Histórico de Chamadas que mostra todas as comunicações para este dispositivo. Para mais informações, consulte "Relatório do Histórico de Chamadas" na página 208.

Relatório de Desvio de Dispositivos por Nome de Dispositivo

O Relatório de Desvio de Dispositivos por Nome do Dispositivo identifica dispositivos que tiveram alterações em seus Nomes de Dispositivo dentro de um intervalo especificado de datas e fornece ligações para informações mais detalhadas sobre dispositivos específicos. É possível especificar critérios de filtro referentes a Nomes de Dispositivos atuais ou anteriores.

NOTA A configuração padrão do Relatório do Desvio de Dispositivos por Nome de Dispositivo pode não mostrar nenhum resultado. Poderá ser necessário definir um intervalo de datas para o relatório apresentar qualquer informação.

Esta seção fornece informações sobre o Relatório do Histórico de Desvio de Dispositivos, que você pode abrir a partir deste relatório.

Para gerar um Relatório de Desvio de Dispositivos por Nome de Dispositivo:

1. Conecte-se à Central do Cliente.

2. No painel de navegação, clique em **Relatórios** > **Histórico de Chamadas e Controle de Perdas** > Relatório **de Desvio de Dispositivo por Nomes de Dispositivos**.
3. No Relatório de Desvio de Dispositivo por Nome de Dispositivo, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione **Nome de Dispositivo**:
   - Clique em **Escolher** para abrir a lista e selecione o dispositivo apropriado.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento é**, abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados pela data, na área **e a alteração ocorreu entre**, faça uma das seguintes ações:
     - No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados.
     - No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.
4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Número de Série**: o número de série deste dispositivo.
   - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
   - **Nome completo do dispositivo Windows**: O nome de domínio totalmente qualificado (FQDN) de um dispositivo, incluindo o nome do dispositivo, o nome de domínio e todos os domínios de nível superior.
   - O link para o **Histórico do Dispositivo** abre o Relatório do Histórico de Desvios do Dispositivo que mostra todas as alterações de um **Identificador** específico aos valores de **Nome de Usuário, Nome de Dispositivo, Hora de Chamada, IP Local (Endereço), ID do Chamador, Domínio, e Grupo de trabalho**.

     Na coluna **Id do Chamador**, clique em um endereço IP para visualizar informações mais detalhadas sobre a ID do chamador. Para mais informações, consulte "Informação de Chamada de IP Estendido" na página 208.

Relatório do Histórico de Desvio de Dispositivos

O relatório do Histórico de Desvio de Dispositivos é um sub-relatório disponível a partir dos relatórios de **Desvio de Dispositivo por Nome de Dispositivo** e **Desvio de Dispositivo por Nome de Usuário**.

O Relatório do Histórico de Desvios mostra todas as alterações de um **Identificador** específico aos valores de **Nome de Usuário**, **Nome de Dispositivo**, **Hora de Chamada**, (Endereço de)**IP Local**, **ID do Chamador**, **Domínio**, e **Grupo de trabalho**.

NOTA O relatório de Histórico de Desvio de Dispositivos**não** está disponível no grupo de relatórios de Histórico de Chamadas e Controle de Perdas.

Para ver o Relatório de Histórico de Desvio de Dispositivos, na grelha de resultados para os relatórios de Desvio de Dispositivo por Nome de Dispositivo ou Desvio de Dispositivo por Nome de Usuário, clique no link **Histórico do Dispositivo**.

Para visualizar informações mais detalhadas sobre o ID do chamador, clique em um endereço IP na coluna **ID de Chamador**. Para mais informações, consulte "Informação de Chamada de IP Estendido" na página 208.

Relatório de Desvio de Dispositivos pelo Usuário

O relatório Desvios de Dispositivos por Nome de Usuário identifica dispositivos cujo Nome de Usuário foi alterado dentro de um intervalo especificado de datas. É possível especificar critérios de filtro referentes a Nomes de Dispositivos atuais ou anteriores.

NOTA Pode ser que a configuração padrão deste relatório não mostre resultados. Talvez seja necessário definir um intervalo de datas para que o relatório apresente alguma informação.

Do Relatório de Desvio de Dispositivos pelo Usuário, é também possível abrir o Relatório do Histórico de Desvio de Dispositivos.

Para gerar um Relatório de Desvio de Dispositivos por Nome de Usuário:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Histórico de Chamadas e Controle de Perdas** > Relatório **de Desvio de Dispositivo por Nome de Usuário**.
3. No Relatório de Desvio de Dispositivo por Nome de Dispositivo, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione **Nome de Usuário**.
   - Clique em **Escolher** para abrir a lista e selecione o dispositivo apropriado.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento é** abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados pela data, na área **e a alteração ocorreu entre**, faça uma das seguintes ações:
     - No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados.

- ○ No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.

   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Número de Série**: o número de série deste dispositivo.
   - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
   - **Nome Completo de Dispositivo Windows**: o nome de domínio totalmente qualificado (FQDN) de um dispositivo, incluindo o nome do dispositivo, o nome de domínio e todos os domínios de nível superior.
   - O link para o **Histórico do Dispositivo** abre o Relatório do Histórico de Desvios do Dispositivo que mostra todas as alterações de um **Identificador** específico aos valores de **Nome de Usuário, Nome de Dispositivo, Hora de Chamada, IP Local (Endereço), ID do Chamador, Domínio, e Grupo de trabalho**.
   - Na coluna **Id do Chamador**, clique em um endereço IP para visualizar informações mais detalhadas sobre a ID do chamador. Consulte "Informação de Chamada de IP Estendido" na página 208.

Relatório de Ativação

O relatório de Ativação identifica, em tempo real, todos os dispositivos que fizeram a primeira chamada para o Centro de Monitoramento dentro de um período de tempo especificado.

NOTA A configuração padrão do relatório de Ativação pode não mostrar nenhum resultado. Pode ser necessário definir o intervalo de datas para a grelha de resultados conter quaisquer informações.

Para gerar um Relatório de Ativação:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Histórico de Chamadas e Controle de Perdas** > **Relatório de Ativação**.
3. No Relatório de Ativação, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:

   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.

     NOTA Dispositivos que foram recentemente ativados podem não estar associados a um grupo de dispositivos. Para mostrar estes dispositivos, selecione **Todos os Dispositivos** na lista **o Grupo é**.

- Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores.
  - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
  - **Nome de Usuário Atribuído:**: O nome de usuário atribuído a um dispositivo por um administrador de sistemas na página Visualizar e Editar Dados de Campos de Definidos pelo Usuário.
  - **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
  - **Número de Série**: o número de série deste dispositivo.
  - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
  - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.

  Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo é ou contém, clique em **Escolher** e selecione um valor da lista.
- Para filtrar seus resultados por Departamento, no campo **e o Departamento é**, abra a lista e selecione o departamento desejado.

  Para retornar um relatório que mostra dispositivos que foram recentemente ativados, selecione a caixa de seleção **Mostrar Ativações Mais Recentes**. Selecionando esta opção desligará o filtro do status da persistência.
- Para filtrar seus resultados pela data, na área **e a Data de Ativação**, faça uma das seguintes ações:
  - No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados.
  - No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.
- Para filtrar resultados por tipo de agente e versão, na área **e o Agente**:

  i) No campo **Tipo** abra a lista e selecione o tipo de agente desejado da seguinte forma:
    - **Qualquer Tipo** retorna um relatório que mostra dispositivos com todos os tipos de agente.
    - **Android** retorna um relatório que mostra apenas dispositivos Android.
    - **BlackBerry** retorna um relatório que mostra apenas dispositivos BlackBerry.
    - **Chromebook** retorna um relatório que mostra apenas dispositivos Chrome para clientes com Computrace Mobile Theft Management (MTM). Para mais informações, consulte "Computrace Mobile Theft Management Mobile Theft Management para Dispositivos Chrome" na página 361.
    - **iOS** retorna um relatório que mostra apenas dispositivos iPad e iPad mini para clientes com Computrace Mobile Theft Management (MTM). Para mais informações, consulte "Computrace Mobile Theft Management para dispositivos iPad" na página 345.
    - **Mac** retorna um relatório que mostra apenas dispositivos Mac.
    - **Windows** retorna um relatório que mostra apenas dispositivos que rodam o sistema operacional Windows.

- ○ **Windows Mobile** retorna um relatório que mostra apenas dispositivos Windows Mobile.

ii) No campo **e versão**, abra a lista e selecione a versão de agente desejada para o **Tipo** de agente que você selecionou anteriormente.

Por exemplo, se você deseja mostrar todos os dispositivos que possuem a versão 898 do agente instalado neles, no campo **tipo**, abra a lista e selecione **Qualquer Tipo** e no campo **e versão** abra a lista e selecione **898**.

IMPORTANTE **SHC** (Chamada de Auto-Reparação) retorna um relatório que mostra dispositivos com agentes que chamaram devido a Persistência. Esta opção aparece quando uma chamada de auto-reparação ocorreu.

- Para filtrar seus resultados pela condição da Tecnologia de Persistência, na área **e o Status de Persistência é**, abra a lista e selecione um dos seguintes valores:
  - **All**: retorna resultados para todos os dispositivos, independentemente de seu estado de Persistência.
  - **BIOS/Firmware Ativo**: retorna resultados para dispositivos com módulos de persistência à base de firmware ativados. A Persistência de firmware está **Ativa** e está fornecendo verificações de agente da integridade de aplicativos quando os dispositivos são reiniciados.
  - **Pendente de BIOS/Firmware**: retorna resultados para dispositivos com módulos de persistência à base de firmware que estão no processo de ativação. Chamadas de agente automáticas adicionais podem ser necessárias antes que este dispositivo faça a transição para o status de **Ativo**.
  - **Software Ativo**: se refere a um dispositivo que possui Persistência de Software, mas que não possui Persistência de BIOS. Com persistência de software, o código do módulo de persistência reside no setor de inicialização mestre do disco rígido, junto do Registro Mestre de Inicialização (RMI). Por exemplo, se você instalasse o agente Computrace em um computador desktop sem persistência de firmware, provavelmente só teria a persistência de software ativa. Quando a persistência de software está ativa, ela fornece verificações de integridade quando o dispositivo é reiniciado.
  - **N/A**: descreve dispositivos que não possuem persistência nenhuma; por exemplo, um computador Mac.

NOTA Antes de poder detectar a Persistência de BIOS/Firmware em um dispositivo ativo, você precisa reinicializar o dispositivo uma vez depois de o mesmo ser ativado e fazer com que ele realize pelo menos duas chamadas de agente.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.

- **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
- **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
- **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
- **Departamento:** o departamento a que pertence este dispositivo.

- **Nome de Usuário Atribuído**: o nome de usuário atribuído a um dispositivo por um administrador de sistemas na página Visualizar e Editar Dados de Campos Definidos pelo Usuário.
- **Marca**: o fabricante de um dispositivo ou outro hardware.

NOTA Para todos os dispositivos Chrome, a marca é **Chromebook**.

- **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
- **Número de Série**: o número de série deste dispositivo.
- **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
- **Data/Hora de Ativação**: a data e a hora que o dispositivo realizou sua primeira chamada para o Centro de Monitoramento.

NOTA Para dispositivos Chrome, esta coluna mostra a data e a hora em que as informações de dispositivo na Central do Cliente foram sincronizadas pela primeira vez com as informações de dispositivo na sua conta do Google.

- **Data/Hora da Última Chamada**: quando o agente instalado em um dispositivo mais recentemente contactou o Centro de Monitoramento.

NOTA Para dispositivos Chrome, esta coluna mostra a data e a hora em que as informações de dispositivo na Central do Cliente foram sincronizadas com as informações de dispositivo na sua conta do Google.

- **Versão**: o número de versão do agente que contata o Centro de Monitoramento.
- **Status de Persistência**: como o agente é restaurado automaticamente quando necessário.
- **Versão do BIOS/Firmware do Sistema**: o nome e número únicos atribuídos ao Sistema Básico de Entrada e Saída (BIOS) de um dispositivo.
- **Data do BIOS/Firmware do Sistema**: a data e a hora que o Sistema Básico de Entrada e Saída (BIOS) instalado em um dispositivo foi lançado.

Relatórios de Rastreamento de Geolocalização

Os relatórios de Rastreamento de Geolocalização incluem o Relatório da Localização do Dispositivo e o Relatório de Histórico da Localização do Dispositivo. Estes relatórios podem ser usados para monitorar as localizações dos seus dispositivos gerenciados usando qualquer uma ou todas das tecnologias de localização suportadas.

IMPORTANTE Apenas Administradores e Usuários Avançados podem ver relatórios de Rastreamento de Geolocalização. Usuários convidados não possuem privilégios de acesso suficientes para acessar os dados de Rastreamento por Geolocalização. A primeira vez que você acessar qualquer página de geolocalização em uma sessão de login, uma página de confirmação solicita que você aceite os Termos e Condições de Uso.

Esta seção oferece informações acerca dos seguintes tópicos:

- Requisitos de Sistema para Geolocalização
- Compreendendo Tecnologias de Localização
- Ativando o Relato de Geolocalização

- Relatório de Localização do Dispositivo
- Relatório de Histórico da Localização do Dispositivo

Requisitos de Sistema para Geolocalização

Você deve instalar uma versão compatível do agente Computrace em dispositivos que deseja que a Central do Cliente rastreie usando a geolocalização.

O recurso de Rastreamento de Geolocalização da Central do Cliente suporta as seguintes plataformas de hardware e software em dispositivos:

- Para Windows:
  - Sistemas Operacionais: para mais informações sobre os requisitos para dispositivos do Windows, consulte "Plataformas Suportadas para o Agente Computrace" na página 22.
  - Versão atual do agente Computrace. Consulte "Baixando o Agente Computrace" na página 127.
  - Se deseja procurar locais usando GPS, você precisa de um receptor de GPS suportado da seguinte lista:

    IMPORTANTE A Central do Cliente suporta a maioria dos receptores GPS disponíveis para dispositivos Windows. A seguinte lista **não** é exaustiva. A Central do Cliente **não** recolhe dados de localização a partir de uma amarra, usando conexões sem fio Bluetooth, USB ou serial, por exemplo para um dispositivo que tem um receptor GPS. Certifique-se de que instale o driver para o receptor de GPS e que o interruptor de sem fios está ativado.

    – Qualcomm UNDP-1 (Gobi 1000) adaptadores de banda larga móvel
    – Qualcomm 9202 adaptador de banda larga móvel
    – Ericsson F3507g e F3607gw adaptadores de banda larga móvel
    – HP un2400 & un2420 adaptadores de banda larga móvel
    – Dell 5600 adaptador de banda larga móvel
  - API de Sensor do Windows e Sensor de Localização (requer Windows 7 ou superior)
  - Se pretende procurar locais usando Wi-Fi, você precisa de um adaptador de rede Wi-Fi.
- Para Mac:
  - Mac OS X 10.5 ou superior
  - Versão 914 do agente Computrace ou posterior. Consulte "Baixando o Agente Computrace" na página 127.
  - Se pretende procurar locais usando Wi-Fi, você precisa de um adaptador de rede Wi-Fi.

  NOTA Core Location **não** é suportado neste momento.
- Dispositivos Móveis (tais como telefones celulares e tablets):
  - Sistemas Operacionais: para mais informações sobre os requisitos para dispositivos móveis, consulte "Plataformas Suportadas para o Agente Computrace" na página 22.
  - Se deseja procurar locais usando GPS, o dispositivo deverá ter um receptor GPS/A-GPS embutido e ativado.
  - Se pretende procurar locais usando a posicionamento Wi-Fi, o dispositivo deve ter um adaptador de rede Wi-Fi embutido que está ativo.

- ○ Se você quiser locais que usam a tecnologia de localização de Estações de Rádio Base ou de Redes, o dispositivo deve suportar este recurso que necessita de ativação.

NOTA O recurso de Rastreamento de Geolocalização da Central do Cliente não é suportado em dispositivos executando o sistema operacional Chrome OS.

Compreendendo Tecnologias de Localização

Esta seção oferece informações acerca dos seguintes tópicos:

- Tipos de Tecnologias de Localização
- Limitações de GPS (Sistemas de Posicionamento Global)
- Limitações da Triangulação Wi-Fi
- Coletando Dados de Localização

Tipos de Tecnologias de Localização

Por ordem de precisão e confiabilidade, informações de localização podem ser coletadas usando qualquer uma das seguintes tecnologias:

Tecnologia de Localização	Descrição
Posicionamento Wi-Fi do Google Maps™	O Posicionamento Wi-Fi do Google Maps determina a localização de um dispositivo ao comparar pontos de acesso Wi-Fi detectados pelo dispositivo com o banco de dados abrangente de pontos de acesso conhecidos da Google e as suas localizações. O dispositivo não precisa de estar conectado ao ponto de acesso Wi-Fi para o ponto de acesso ser detectado. Esta tecnologia é mais eficaz em zonas urbanas onde pontos de acesso Wi-Fi são abundantes. Ele funciona com dispositivos Windows e Mac, Windows Mobile e dispositivos móveis Android. Para usar o Posicionamento Wi-Fi do Google Maps, uma configuração precisa ser ativada na sua conta. Para informações sobre como ativar esta configuração, consulte "Editando Configurações de Conta" na página 116. **NOTA** Se um dispositivo gerenciado estiver em um país onde o Google Maps seja proibido, o Posicionamento Wi-Fi do Google Maps não poderá ser usado para resolver a localização do dispositivo.
Sistemas de Posicionamento Global (GPS)	A tecnologia de Sistemas de Posicionamento Global (GPS) determina a localização de um dispositivo usando sensores incorporados para capturar sinais de satélite que indicam o local do dispositivo. GPS é mais eficaz quando o dispositivo está ao ar livre. Esta tecnologia funciona com dispositivos Windows e BlackBerry, Windows Mobile e dispositivos móveis Android que estão equipados com um receptor GPS compatível.

Tecnologia de Localização	Descrição
Outras Tecnologias de Localização	Inclui as seguintes tecnologias: ● **API**, tal como o Microsoft Windows Sensor e API do Sensor de Localização, usam uma série de métodos para identificar a localização de dispositivos. Esta tecnologia funciona com dispositivos Windows. ● **Celular**, identifica localizações de dispositivos usando tecnologia de localização por torre/rede celular. Esta informação é tipicamente determinada usando técnicas de triangulação que são baseadas em localizações conhecidas de estações baseadas em 2G, 3G e 4G e/ou localizações de redes Wi-Fi (sem-fios). Estes locais conhecidos são mantidos pelo fabricante do dispositivo ou pela operadora de rede móvel. Esta tecnologia funciona com dispositivos móveis Android.
Posicionamento Wi-Fi Absolute	O posicionamento Wi-Fi Absolute determina a localização de um dispositivo ao comparar pontos de acesso Wi-Fi detectados pelo dispositivo com o banco de dados de pontos de acesso conhecidos da Absolute e as suas localizações. O dispositivo não precisa estar conectado ao ponto de acesso Wi-Fi para o ponto de acesso ser detectado. Esta tecnologia é mais eficaz em zonas urbanas onde pontos de acesso Wi-Fi são abundantes. Ele funciona com dispositivos Windows e Mac, Windows Mobile e dispositivos móveis Android.
Georesolução IP	A georesolução IP usa um banco de dados de endereços IP e suas localizações para determinar a localização de um dispositivo. Esta tecnologia é habitualmente precisa a nível de país, mas as localizações de dispositivos dentro de regiões ou cidades são menos confiáveis. Esta tecnologia funciona com dispositivos Windows e Mac, BlackBerry, Windows Mobile e dispositivos móveis Android.

Limitações de GPS (Sistemas de Posicionamento Global)

Os receptores GPS são projetados para receber um sinal de satélites de forma confiável quando eles estão ao ar livre, com uma visão desobstruída do céu. Por isso, é improvável que os receptores GPS funcionem bem quando rodeados por edifício altos ou dentro de edifícios com estruturas de metal ou concreto. Os receptores GPS podem funcionar dentro de edifícios sem estrutura metálica ou perto de janelas.

A precisão da localização relatada pelo GPS depende de questões ambientais, tais como a quantidade de satélites à vista, o potencial reflexo dos sinais de satélite em objetos próximos ou efeitos atmosféricos. Em condições ideais, o GPS disponível normalmente relata localizações dentro de 10 m do local real. Quando as condições são menos favoráveis, o erro pode aumentar para até 100 m ou mais. As coordenadas GPS provavelmente não são exatas.

Limitações da Triangulação Wi-Fi

A triangulação Wi-Fi é um método de rastreamento correlacional baseado nas localizações por GPS conhecidas de pontos de acesso Wi-Fi detectados na proximidade de um dado dispositivo. A intensidade mensurada da rede Wi-Fi ajuda determinar a proximidade do dispositivo a um determinado ponto de acesso. Geralmente o posicionamento Wi-Fi fornece uma localização com a precisão de até alguns quarteirões de distância.

Coletando Dados de Localização

Para todas as tecnologias de localização, exceto o Posicionamento Wi-Fi do Google Maps e a Georesolução de IP, dados de localização são coletados de hora em hora e são carregados para a Central do Cliente cada vez que o dispositivo faz uma chamada para o Centro de Monitoramento (normalmente uma vez por dia). Para o Posicionamento Wi-Fi do Google Maps e a Georesolução IP, localizações são coletadas cada vez que o dispositivo chama o Centro de Monitoramento.

NOTA Se você deseja carregar uma localização cada vez que um dispositivo altere a sua localização, é possível ativar as Chamadas de Eventos para os seus dispositivos do Windows e Mac gerenciados. Para mais informações, consulte "Gerenciando Chamadas de Eventos para Sua Conta" na página 119.

Os usuários finais de um dispositivo podem desativar a tecnologia de localização; por exemplo, os usuários podem desativar o GPS ou Wi-Fi para todos os aplicativos. Para coletar informações de localização, pelo menos uma das tecnologias de localização devem estar ativas no dispositivo.

Ativando o Relato de Geolocalização

Por padrão, os relatórios de Localização de Dispositivos e de Históricos de Localização de Dispositivos não são ativados em sua conta da Central do Cliente. Você deve enviar um Formulário de Autorização de Geolocalização antes da ativação dos relatórios.

NOTA Dados de localização são recolhidos somente para dispositivos equipados com o recurso de Rastreamento por Geolocalização. Para uma lista de hardware e software necessários para a Central do Cliente poder coletar informações de geolocalização de um dispositivo, consulte "Requisitos de Sistema para Geolocalização" na página 218.

Para ativar o Relatório de Geolocalização na Central do Cliente:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique no link para **Documentação**.
3. Na área **Formulários de Solicitação de Serviço**, clique no **Formulário de Autorização do Administrador de Segurança e do Rastreamento por Geolocalização**.
4. Preencha e envie o formulário para o número de fax do Suporte Global da Absolute listado no formulário. O Suporte Global notifica você quando o recurso de Relatórios de Geolocalização for ativada para a sua conta.

Relatório de Localização do Dispositivo

O Relatório de Localização de Dispositivos mostra as localizações geográficas mais recentes, também conhecidas por geolocalizações, de dispositivos, com base em tecnologia de geolocalização disponível em dispositivos quando estes relatam uma localização.

Para gerar um Relatório de Localização de Dispositivos:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.
2. No painel de navegação, clique em **Relatórios** > **Histórico de Chamadas e Controle de Perdas** > **Relatório de Localização de Dispositivo**. A página Rastreamento por Geolocalização se abre.

3. Na página Rastreamento de Geolocalização, clique em **Aceitar** para aceitar os termos e as condições do Contrato de Serviço.
4. No Relatório de Localização de Dispositivos, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores.
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
     - **Marca**: o fabricante de um dispositivo ou outro hardware.
     - **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
     - **Número de Série**: o número de série deste dispositivo.
     - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
     - **Nome de Usuário Atribuído**: o nome de usuário atribuído ao dispositivo por um administrador de sistemas.
     - **Fornecedor do Contrato de Garantia**: o prestador de garantia para um dispositivo.

     Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo é ou contém, clique em **Escolher** e selecione um valor da lista.
   - Para filtrar seus resultados por data, na área **e quando o**, faça uma das seguintes ações:
     - No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados
     - No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.
   - Para filtrar resultados por tipo de agente e versão, na área **e o Agente**:

     i) No campo **Tipo** abra a lista e selecione o tipo de agente desejado da seguinte forma:
       - **Qualquer Tipo** retorna um relatório que mostra dispositivos com todos os tipos de agente.
       - **Android** retorna um relatório que mostra apenas dispositivos Android.
       - **BlackBerry** retorna um relatório que mostra apenas dispositivos BlackBerry.
       - **Mac** retorna um relatório que mostra apenas dispositivos Mac.
       - **Windows** retorna um relatório que mostra apenas dispositivos que rodam o sistema operacional Windows.
       - **Windows Mobile** retorna um relatório que mostra apenas dispositivos Windows Mobile.

NOTA Se você selecionar **Chromebook** nenhuns resultados serão retornados porque a geolocalização não é suportada.

ii) No campo **e versão**, abra a lista e selecione a **Versão** de agente desejada para o **Tipo** de agente que você selecionou anteriormente.

Por exemplo, se você deseja mostrar todos os dispositivos que possuem a versão 898 do agente instalado neles, no campo **tipo**, abra a lista e selecione **Qualquer Tipo** e no campo **versão** abra a lista e selecione **898**.

NOTA **SHC** (Chamada de Auto-Reparação) retorna um relatório que mostra dispositivos com agentes que chamaram devido à Persistência. Esta opção aparece quando uma chamada de auto-reparação ocorreu.

- Para filtrar seus resultados por Departamento, no campo **e o Departamento é**, abra a lista e selecione o departamento desejado.
- Para filtrar os resultados por status de agente, no campo **e o Status é**, abra a lista e selecione uma das seguintes opções.
  - **Tudo** mostra aqueles dispositivos especificados em que a condição de operação do agente é Ativa, Inativa ou Desativada.
  - **Ativo** mostra apenas aqueles dispositivos cujo agente chamou para o Centro de Monitoramento.
  - **Inativo** mostra apenas aqueles dispositivos cujo agente ainda não chamou para o Centro de Monitoramento.
  - **Desativado** mostra apenas aqueles dispositivos cujo agente está sinalizado para remoção ou removido do dispositivo.
- Para filtrar seus resultados por Localização, na área **e a Localização**, abra a lista e selecione uma ou ambas as seguintes opções:
  - **Mostrar apenas locais com altos níveis de confiança.**
  - **Mostrar apenas um máximo de 500 locais**
- Para filtrar seus resultados por Tecnologia de Localização, na área **e a Localização foi obtida via**, abra a lista e selecione uma das seguintes opções:
  - **Posicionamento Wi-Fi do Google Maps™**

    Se esta opção estiver acinzentada, então esta tecnologia de localização não está disponível porque a configuração **Usar Geolocalização da Google para Pontos de Acesso Wi-Fi** não está ativa na sua conta. Para informações sobre como ativar esta configuração, consulte "Editando Configurações de Conta" na página 116.

    Se esta opção não for exibida, o Google Maps e a sua tecnologia de localização são proibidos no seu país (determinado pelo endereço IP do seu computador).
  - **GPS**
  - **Outras Tecnologias de Localização**
  - **Posicionamento Wi-Fi Absolute**
  - **Georesolução IP**

  Para mais informações sobre cada tecnologia de localização, consulte "Tipos de Tecnologias de Localização" na página 219.

5. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.

   Na grelha de resultados, os dispositivos equipados com Rastreamento por Geolocalização aparecem como ícones no mapa. Todos os limites de Cercas Geográficas da sua conta também são exibidos.

   É possível navegar pelo mapa usando as seguintes ferramentas:

Ferramenta	**Descrição**
Movimento Panorâmico	Use a ferramenta de movimentos panorâmicos para uma área específica do mapa. Clique em uma ou mais das setas até a área desejada estar em vista. Esta ferramenta é tipicamente usada em conjunto com a ferramenta de Zoom.
Zoom	Use a ferramenta de Zoom para ampliar ou reduzir áreas específicas do mapa. ● Para ampliar, clique em [+] repetidamente, ou desloque o controle deslizante em direção ao botão. É também possível ampliar o zoom clicando duas vezes no mapa ou usando a roda de rolagem de seu mouse. ● Para reduzir o zoom, clique em [−] repetidamente, ou desloque o controle deslizante em direção ao botão. É possível reduzir o zoom ao usar a roda de rolagem de seu mouse.
Mapa | Selecionador de Satélite	Usar o mapa | Ferramenta de satélite para selecionar o tipo de mapa. Para selecionar um tipo de mapa, execute uma das seguintes ações: ● Para mostrar um mapa de ruas, clique em **Mapa**. Esta é a opção padrão. ● Para mostrar um mapa com informações de relevo e vegetação, clique em **Mapa** e selecione **Relevo**. ● Para mostrar um mapa de imagens de satélite, clique em **Satélite**. ● Para mostrar um mapa de imagens de satélite com nomes de localidades, clique em **Satélite** e selecione **Etiquetas**.
Ir para o endereço	Use a ferramenta Ir para Endereço para visualizar uma localização específica no mapa. Para encontrar um local, clique no ícone, insira o endereço do local no campo fornecido e pressione `Enter`. Para obter maior precisão, forneça uma morada física, bem como nomes de cidade e estado.
Encontrar limites e marcadores	Se múltiplos limites aparecem num mapa, use a ferramenta Localizar Limites e Marcadores para ver os limites individualmente. Clique no ícone repetidamente para percorrer cada limite e marcador no mapa.

NOTA O mapa de geolocalização no Relatório de Localização do Dispositivo é um mapa do Google Maps. Se o Google Maps é proibido no seu país (determinado pelo endereço IP do seu computador), um mapa ESRI® aparece em vez. Para mais informações sobre como usar os mapas ESRI, vá para www.esri.com.

Cada tipo de tecnologia de localização mostra um ícone específico no mapa:

Posicionamento Wi-Fi do Google Maps

NOTA Se um dispositivo estiver em um país onde o Google Maps seja proibido, esta tecnologia não poderá ser usada para resolver a localização do dispositivo.

Sistema de Posicionamento Global

Computadores usando outras tecnologias de localização, tal como a API

Dispositivos Móveis usando outras tecnologias de localização, tal como a celular

Posicionamento Wi-Fi Absolute

Georesolução IP

Um pequeno número no canto superior direito de um ícone indica o número de dispositivos na área do mapa abaixo do ícone. Se todos os dispositivos na área do mapa abaixo do ícone usam o mesmo tipo de tecnologia de localização, o ícone exibe a tecnologia de localização. Caso contrário, o ícone não exibe tecnologia de localização.

6. Clique em um ícone para abrir uma caixa de diálogo contendo um link de **Ampliar Zoom** para ver o local, bem como as seguintes informações sobre dispositivos que o ícone representa:
   - **Identificador**: o número de identificação único associado ao dispositivo.
   - **Nome do Dispositivo** é o nome atribuído a este dispositivo no sistema operacional.
   - **Nome de Usuário** é o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
   - **Marca** é o nome do fabricante do dispositivo como capturado pelo agente.
   - **Modelo** é o número de modelo do dispositivo tal como o agente o capturou.
   - **Localização** é um link que permite a você fazer zoom e se aproximar da última localização conhecida do dispositivo.
   - **Hora da Localização** é a data e a hora da última localização conhecida do dispositivo. Clicando no link **Histórico** abre a página Relatórios de Históricos de Localização para o dispositivo.
   - **Tecnologia de Localização** é a tecnologia usada para determinar a localização do equipamento.
7. A grelha de resultados abaixo do mapa fornece informações de local completas para cada dispositivo. Clique em um link na coluna **Última Localização Conhecida (Latitude, Longitude)** para ver a localização de um dispositivo no mapa.

Para mais informações sobre como usar a geotecnologia da Central do Cliente, consulte "Gerenciando Cercas Geográficas" na página 296.

Relatório de Histórico da Localização do Dispositivo

IMPORTANTE Somente Administradores e Usuários Avançados podem visualizar os Relatórios de Localização de Dispositivos e de Histórico de Localização de Dispositivos. Usuários convidados não possuem privilégios de acesso suficientes para acessar os dados de Rastreamento por Geolocalização. A primeira vez que você acessar qualquer página de geolocalização em uma sessão de login, uma página de confirmação solicita que você aceite os Termos e Condições de Uso.

O Relatório do Histórico da Localização do Dispositivo rastreia a localização de um único dispositivo, ao longo do tempo, usando a melhor tecnologia de localização disponível quando o dispositivo comunicou uma localização. Para uma lista de tecnologias de localização disponíveis, ordenadas por exatidão e confiabilidade, consulte "Tipos de Tecnologias de Localização" na página 219.

A posição de um dispositivo ao longo do tempo é representada como um conjunto de ícones em um mapa. A cor do ícone indica o período de tempo da informação. As localizações mais recentes são vermelhas, enquanto as localizações relatadas no passado esmaecem e passam de vermelho para branco assim que envelhecem. Clicando em um ícone abre uma caixa de diálogo contendo detalhes sobre os dispositivos que o ícone representa.

Informações na grelha de resultados que aparece abaixo do mapa representam coordenadas de latitude e longitude, medidas em graus decimais.

Para mais informações sobre como usar a geotecnologia da Central do Cliente, consulte "Gerenciando Cercas Geográficas" na página 296.

Para gerar um Relatório do Histórico da Localização de Dispositivos:

1. Entre na Central do Cliente como um Administrador ou Usuário Avançado.
2. No painel de navegação, clique em **Relatórios** > **Histórico de Chamadas e Controle de Perdas** > **Relatóriodo Histórico da Localização de Dispositivos**.
3. No Relatório do Histórico da Localização de Dispositivos, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Dispositivo, no campo **o Dispositivo é**, clique em **Escolher** para abrir a lista e selecionar o grupo de dispositivos desejado.
   - Para filtrar seus resultados por data, na área **e uma Localização foi determinada entre**, faça uma das seguintes ações:
     - No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados.
     - No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do calendário para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.
   - Para filtrar seus resultados por Localização, na área **e a Confiança é**, selecione uma ou ambas as seguintes opções:
     - **Mostrar apenas locais com altos níveis de confiança.**
     - **Mostrar apenas um máximo de 500 locais**
   - Para filtrar seus resultados por tecnologia de localização, na área **e a Localização foi obtida via**, selecione uma ou várias das seguintes opções:
     - **Posicionamento Wi-Fi do Google Maps™**
       Se esta opção estiver acinzentada, então esta tecnologia de localização não está disponível porque a configuração **Usar Geolocalização da Google para Pontos de Acesso Wi-Fi** não está ativa na sua conta. Para informações sobre como ativar esta configuração, consulte "Editando Configurações de Conta" na página 116. Se esta opção não for exibida, o Google Maps e a sua tecnologia de localização são proibidos no seu país (determinado pelo endereço IP do seu computador).

- **GPS**
- **Outras Tecnologias de Localização**
- **Posicionamento Wi-Fi Absolute**
- **Georesolução IP**

Para mais informações sobre cada tecnologia de localização, consulte "Tipos de Tecnologias de Localização" na página 219.

- Clique no campo **e mostrar local** e selecione uma das seguintes opções para indicar o âmbito dos dados de localização a incluir no relatório:
  - **entre chamadas (todas as localizações intermediárias conhecidas)**
  - **na última chamada (última localização conhecida na última chamada)**

NOTA Se você selecionar apenas a opção de Posicionamento Wi-Fi do Google Maps™ na etapa anterior, a opção **na última chamada** será selecionada por padrão e não poderá ser alterada. Esta tecnologia de localização coleta dados de localização apenas durante chamadas de agente.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.

Na grelha de resultados, as localizações dos dispositivos aparecem como ícones no mapa. Todos os limites de Cercas Geográficas da sua conta também são exibidos.

É possível navegar pelo mapa usando as seguintes ferramentas:

Ferramenta	Descrição
Movimento Panorâmico	Use a ferramenta de movimentos panorâmicos para uma área específica do mapa. Clique em uma ou mais das setas até a área desejada estar em vista. Esta ferramenta é tipicamente usada em conjunto com a ferramenta de Zoom.
Zoom	Use a ferramenta de Zoom para ampliar ou reduzir áreas específicas do mapa. ● Para ampliar o zoom, clique em + repetidamente, ou desloque o controle deslizante em direção ao botão. É também possível ampliar o zoom clicando duas vezes no mapa ou usando a roda de rolagem de seu mouse. ● Para reduzir o zoom, clique em − repetidamente, ou desloque o controle deslizante em direção ao botão. É possível reduzir o zoom ao usar a roda de rolagem de seu mouse.
Mapa | Selecionador de Satélite	Usar o mapa | Ferramenta de satélite para selecionar o tipo de mapa. Para selecionar um tipo de mapa, execute uma das seguintes ações: ● Para mostrar um mapa de ruas, clique em **Mapa**. Esta é a opção padrão. ● Para mostrar um mapa com informações de relevo e vegetação, clique em **Mapa** e selecione **Relevo**. ● Para mostrar um mapa de imagens de satélite, clique em **Satélite**. ● Para mostrar um mapa de imagens de satélite com nomes de localidades, clique em **Satélite** e selecione **Etiquetas**.

Ferramenta	Descrição
Ir para o endereço	Use a ferramenta Ir para Endereço para visualizar uma localização específica no mapa. Para encontrar um local, clique no ícone, insira o endereço do local no campo fornecido e pressione `Enter`. Para obter maior precisão, forneça uma morada física, bem como nomes de cidade e estado.
Encontrar limites e marcadores:	Se múltiplos limites aparecem num mapa, use a ferramenta Localizar Limites e Marcadores para ver os limites individualmente. Clique no ícone repetidamente para percorrer cada limite e marcador no mapa.

NOTA O Relatório de Histórico da Localização do Dispositivo usa o Google Maps. Se o Google Maps é proibido no seu país (determinado pelo endereço IP do seu computador), um mapa ESRI® aparece em vez. Para mais informações sobre como usar os mapas ESRI, vá para www.esri.com.

Cada tipo de tecnologia de localização mostra um ícone específico no mapa:

Posicionamento Wi-Fi do Google Maps

NOTA Se um dispositivo se localizar em um país onde o Google Maps seja proibido, esta tecnologia não poderá ser usada para resolver a localização do dispositivo.

Sistema de Posicionamento Global

Computadores usando outras tecnologias de localização, tal como a API

Dispositivos Móveis usando outras tecnologias de localização, tal como a celular

Posicionamento Wi-Fi Absolute

Georesolução IP

Um pequeno número no canto superior direito de um ícone indica o número de localizações na área do mapa abaixo do ícone. Se todas as localizações usaram o mesmo tipo de tecnologia de localização, o ícone mostra a tecnologia de localização. Caso contrário, o ícone não exibe tecnologia de localização.

5. Clique em um ícone para abrir uma caixa de diálogo contendo um link de **Ampliar Zoom** para ver o local do ícone, bem como as seguintes informações:
   - **Hora da Localização**: a data e hora da última localização conhecida do dispositivo.
   - **Localização**: o link que permite a você fazer zoom e se aproximar da última localização conhecida do dispositivo
   - **Tecnologia de Localização**: a tecnologia usada para determinar a localização do equipamento.
6. A grelha de resultados abaixo do mapa fornece detalhes completos sobre as localizações do dispositivo. Clique em um link na coluna **Localização (Latitude, Longitude)** para ver uma localização específica no mapa.

Relatórios de Gerenciamento de Inventário e de Concessão

Esta seção fornece informação sobre os seguintes relatórios:

- Relatório de Conclusão de Contrato de Locação
- Dados Digitados pelo Usuário

Relatório de Conclusão de Contrato de Locação

O relatório da Conclusão da Concessão identifica todos os ativos no qual a concessão expira em um determinado período de tempo. O relatório de conclusão da concessão não exibe campos com valores nulos.

Por padrão, a saída do Relatório de Conclusão de Contrato de Concessão inclui dispositivos que têm um contrato que expira dentro de 30 dias. É possível alterar o intervalo de datas a incluir na grelha de resultados.

NOTA Para instruções detalhadas sobre a inserção de informações sobre novas concessões ou a atualização de informações de concessões existentes, consulte "Dados" na página 53.

Para gerar o Relatório de Conclusão da Concessão:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Gerenciamento de Inventários e de Concessões** > **Relatório de Conclusão de Concessão**.
3. Na página Relatórios de Conclusão de Concessão, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
     - **Nome de Usuário Atribuído**: o nome de usuário atribuído ao dispositivo por um administrador de sistemas.
     - **Centro/Código de Custos**: um identificador único para uma unidade para qual os custos são acumulados ou computados.
     - **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
     - **Endereço IP**: um número único que identifica um dispositivo na Internet.
     - **Número de Concessão**: um identificador único atribuído a uma concessão.
     - **Responsabilidade da Concessão**: a parte responsável pelos bens locados.
     - **Vendedor da Concessão**: o fornecedor de bens locados. Nem todos os locadores de equipamentos fornecem manutenção e suporte de serviços. Por esta razão, é possível que o fornecedor da concessão e o fornecedor do serviço não sejam os mesmos e as datas de contrato sejam diferentes.
     - **Referência de Ordem de Compra**: um identificador único associado a uma autorização para adquirir bens ou serviços.

- ○ **Número de Série**: o número de série deste dispositivo.
- ○ **Contrato de Serviço**: uma prestação de suporte e manutenção de ativos.
- ○ **Telefone/Extensão do Usuário**: o número de telefone completo de uma pessoa associada a um dispositivo.
- ○ **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
- ○ **Fornecedor do Contrato de Garantia**: o prestador de garantia para um dispositivo.
- ○ **Localização Física/Real**: onde o dispositivo reside.
- ○ Quaisquer **Campos Definidos pelo Usuário (CDU)** que você pode ter definido estão listados aqui e você pode usá-los para filtrar seu relatório. Um UDF é um atributo para um dispositivo que um usuário da Central do Cliente pode criar e editar.

Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo é ou contém, clique em **Escolher** e selecione um valor da lista.

- Para filtrar seus resultados por data, na área **e a data do Fim da Concessão é**, faça uma das seguintes ações:
  - ○ No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados.
  - ○ No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.
- Para filtrar seus resultados por data em um contrato de cliente, na área **e quando o**:

  i) Abra a lista e selecione uma das seguintes opções:
  - ○ **Data do fim da concessão**
  - ○ **Data de início do contrato de concessão**
  - ○ **Data de Terminação do Contrato de Serviço**
  - ○ **Data de Início do Contrato de Serviço**
  - ○ **Data de Terminação da Garantia**
  - ○ **Data de Início da Garantia**
  - ○ **Data de Aquisição do Dispositivo**

  ii) No campo **é**, selecione uma das seguintes opções:
  - ○ **Antes**
  - ○ **Em ou depois**
  - ○ **Ligado**

  iii) Digite a data (dd/mm/aaaa) ou clique no ícone do **Calendário** para selecioná-la.

  Por padrão, a saída do Relatório de Conclusão de Contrato de Concessão inclui dispositivos que têm um contrato que expira dentro de 30 dias.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.

   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.

- **Nome do Campo**: o nome do campo definido pelo usuário usado para filtrar o relatório na etapa 3.
- **Valor do Campo**: o valor do campo definido pelo usuário usado para filtrar o relatório na etapa 3.
- **Departamento**: o departamento a que pertence este dispositivo
- **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
- **Marca**: o fabricante de um dispositivo ou outro hardware.
- **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
- **Número de Série**: o número de série deste dispositivo.
- **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.

Dados Digitados pelo Usuário

O relatório de Dados Digitados pelo Usuário permite a visualização de todos os dados manualmente inseridos associados a seus dispositivos rastreados, o que inclui todos os dados armazenados em campos definidos pelo usuário (UDFs - User-Defined Fields) e pontos de dados que o agente não consegue capturar automaticamente.

NOTA Para uma discussão completa de UDFs, consulte "Exportando e Importando Dados" na página 57.

Esta seção fornece as seguintes tarefas:

- Gerando um Relatório de Dados Digitados pelo Usuário
- Selecionando os Pontos de Dados Que Você Deseja Ver

Gerando um Relatório de Dados Digitados pelo Usuário

Para gerar um Relatório de Dados Digitados pelo Usuário:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Gerenciamento de Inventários e de Concessões** > **Relatório de Dados Digitados pelo Usuário**.
3. No Relatório de Dados Digitados pelo Usuário, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores:
     - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
     - **Nome de Usuário Atribuído**: o nome de usuário atribuído ao dispositivo por um administrador de sistemas.

- **Centro/Código de Custos**: um identificador único para uma unidade para qual os custos são acumulados ou computados.
- **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
- **Data de Aquisição do Dispositivo**: a data em que o dispositivo foi adquirido.
- **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
- **Data de Instalação**: a data e a hora da primeira chamada de agente para o Centro de Monitoramento.
- **Número de Concessão**: um identificador único atribuído a uma concessão.
- **Responsabilidade da Concessão**: a parte responsável pelos bens locados.
- **Vendedor da Concessão**: o fornecedor de bens locados. Nem todos os locadores de equipamentos fornecem manutenção e suporte de serviços. Por esta razão, é possível que o fornecedor da concessão e o fornecedor do serviço não sejam os mesmos e as datas de contrato sejam diferentes.
- **Referência de Ordem de Compra**: um identificador único associado a uma autorização para adquirir bens ou serviços.
- **Número de Série**: o número de série deste dispositivo.
- **Data Final do Contrato de Serviço**: quando a prestação de suporte e manutenção de ativos acaba.
- **Data de Início do Contrato de Serviço**: quando a prestação de suporte e manutenção de ativos começa.
- **Vendedor de Contrato de Serviço**: o nome do fornecedor de suporte e manutenção de ativos.
- **Telefone/Extensão do Usuário**: o número de telefone completo de uma pessoa associada a um dispositivo.
- **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
- **Fornecedor do Contrato de Garantia**: o prestador de garantia para um dispositivo.
- **Localização Física/Real**: a localização de dispositivo descrita no campo definido pelo usuário.
- Quaisquer **Campos Definidos pelo Usuário (CDU)** que você pode ter definido estão listados aqui e você pode usá-los para filtrar seu relatório. Um UDF é um atributo para um dispositivo que um usuário da Central do Cliente pode criar e editar.

Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.

- Para filtrar seus resultados por data, na área **e quando** :

  i) Abra a lista e selecione uma das seguintes opções:
    - **Data de Aquisição do Dispositivo**
    - **Data de Instalação**
    - **Data do fim da concessão**
    - **Data de início do contrato de concessão**
    - **Data de Terminação do Contrato de Serviço**
    - **Data de Início do Contrato de Serviço**
    - **Data de Terminação da Garantia**

- **Data de Início da Garantia**

ii) Faça uma das seguintes opções:

- No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resultará em um relatório maior e levará mais tempo a gerar resultados.
- No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.

- Para filtrar seus resultados por departamento, no campo **e o Departamento**, abra a lista e selecione o departamento desejado.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.
   - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo deste dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
   - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
   - **Nome do Dispositivo**: o nome atribuído a este dispositivo no sistema operacional.
   - **Endereço IP**: um número único que identifica um dispositivo na Internet.

Selecionando os Pontos de Dados Que Você Deseja Ver

Para selecionar que pontos de dados aparecem na grelha resultados:

1. Complete a tarefa, "Gerando um Relatório de Dados Digitados pelo Usuário" na página 231.
2. Na grelha de resultados, clique em **Escolher Colunas**.
3. No diálogo de Campos Personalizados, selecione o campo desejado no painel de Campos Disponíveis, e depois clique em **>** para adicionar o campo ao painel de Campos Selecionados. Para adicionar todos os campos, clique em **>>**.

   Para remover um campo da grelha de resultados, selecione o campo no painel Campos Selecionados , e depois clique em **<.** Para remover todos os campos, clique em **<<**.
4. Repita Etapa 3 conforme necessário para preparar o formato da grelha de resultados.
5. Clique em **OK** para retornar à página do Relatório de Dados Digitados pelo Usuário.

Relatórios de Gerenciamento de Contas

É possível usar os relatórios de Gerenciamento de Conta para monitorar e rastrear licenças de agentes pertencendo à sua empresa e para ajudar a resolver problemas de licenciamento.

NOTA Os usuários convidados não podem acessar a área de Relatórios de Gerenciamento de Contas e, portanto, não podem ver quaisquer relatórios aí contidos.

Esta seção fornece informação sobre os seguintes relatórios:

- Relatório do Resumo do Uso de Licenças

- Relatório de Perfis de Chamadas
- Relatório de Auditoria do Usuário
- Relatório de Eventos de Usuário

Relatório do Resumo do Uso de Licenças

O Relatório do Resumo do Uso de Licenças fornece detalhes sobre o status atual do licenciamento de sua conta da Central do Cliente, incluindo a taxa de instalação.

Para baixar o Relatório de Resumo de Uso de Licenças:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Gerenciamento de Contas** > **Relatório do Resumo do Uso da Licença**.
3. No relatório do resumo do uso da licença, no campo **Nome**, digite um nome único para seu relatório.
4. No campo **Formato**, abra a lista e selecione uma das seguintes opções:
   - **CSV**: um arquivo de texto simples com colunas separadas por vírgula que é aberto com software incluído no seu sistema operacional. Recomendado para consultas SQL e o carregamento de arquivos de dados grandes.
   - **XML:** um arquivo de linguagem que é aberta com um editor de XML, tal como o Microsoft Excel ou OpenOffice. Recomendado para a filtragem e a formatação de dados.
5. No local de Criar Alerta de E-mail, no campo **Seu Endereço de E-mail**, digite seu endereço de e-mail se você deseja receber uma notificação por e-mail quando o relatório estiver processado.
6. Clique no botão **Continuar** para colocar o download em fila.
7. Quando sua solicitação for processada, você pode obter o arquivo CSV ou XML do relatório na página **Meus Relatórios**. Para mais informações, consulte "Baixando Relatórios" na página 150.

   O download do Resumo de Uso de Licenças inclui os seguintes dados:
   - **AbsoluteTrack**: número total de licenças do AbsoluteTrack compradas.
   - **Computrace Complete**: número total de licenças adquiridas do Computrace Complete.
   - **Total de Licenças**: total combinado de licenças do AbsoluteTrack e do Computrace Complete adquiridas.
   - **Total Instalado**: total combinado de todas as licenças do AbsoluteTrack e do Computrace Complete instaladas em sua conta.
   - **Instalações em Excesso (-) ou em Falta (+)**: número total de licenças adquiridas, menos o número total de licenças instaladas.
   - **Taxa de Instalação**: percentual de licenças compradas que foram instaladas.
   - **Chamadas dos Últimos 30 Dias**: total combinado de licenças que chamaram o Centro de Monitoramento nos últimos 30 dias.
   - **Taxa de Chamada Recente**: o valor acima como um percentual
   - **Garantia de Serviço Instalada**: número total de licenças de Garantias de Serviço Instaladas
   - **Instalações em Excesso (-) ou em Falta (+)**: total de licenças de Garantia de Serviço compradas, menos o total de licenças de Garantia de Serviço instaladas.

- **Taxa de Instalação**: percentagem de licenças de Garantia de Serviço compradas que foram instaladas.
- **Chamadas dos Últimos 30 Dias**: total de licenças de Garantia de Serviço que chamaram o Centro de Monitoramento nos últimos 30 dias.
- **Taxa de Chamadas Recebidas Recentes**: número total de licenças de Garantia de Serviço que chamaram o Centro de Monitoramento nos últimos 30 dias, representado como percentual.

Relatório de Perfis de Chamadas

O Relatório de Perfis de Chamadas fornece informações detalhadas sobre os padrões de chamadas de cada dispositivo.

Para baixar o relatório de Perfis de Chamada:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Gerenciamento de Contas** > **Relatório dos Perfis de Chamadas**.
3. Na página Relatórios dos Perfis de Chamadas, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
   - Para filtrar seus resultados por Departamento, no campo **e o Departamento**, abra a lista e selecione o departamento desejado.
   - Para filtrar seus resultados por dispositivo específico, na área **e o campo**, abra a lista e selecione um dos seguintes valores.
     - **Quaisquer dos campos nesta lista**: seleciona todos os valores na lista.
     - **Identificador**: um Número de Série Eletrônico único atribuído ao agente instalado em um dispositivo.
     - **Nome de dispositivo**: o nome atribuído ao dispositivo no sistema operacional.
     - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo.
     - **Número de Série**: o número de série deste dispositivo.
     - **Número de Ativo**: o número de identificação associado a um dispositivo na Central do Cliente.
     - **Marca**: o fabricante de um dispositivo ou outro hardware.

       NOTA Para todos os dispositivos Chrome, a marca é **Chromebook**.
     - **Modelo**: o tipo de produto de um dispositivo ou outro hardware.
     - **Nome de Usuário Atribuído**: o nome de usuário atribuído ao dispositivo por um administrador de sistemas.

   Dependendo do valor que você selecionou da lista precedente, você pode querer definir ainda mais este campo. No campo **é ou contém**, clique em **Escolher** e selecione um valor da lista.

4. Para filtrar seus resultados por Grupo de Dispositivos, no campo **o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado.
5. Na área de **Nome e Formato**, no campo **Nome**, digite um nome único para seu relatório.
6. No campo **Formato**, abra a lista e selecione uma das seguintes opções:
   - **CSV**: um arquivo de texto simples com colunas separadas por vírgula que é aberto com software incluído no seu sistema operacional. Recomendado para consultas SQL e o carregamento de arquivos de dados grandes.
   - **XML:** um arquivo de linguagem que é aberta com um editor de XML, tal como o Microsoft Excel ou OpenOffice. Recomendado para a filtragem e a formatação de dados.
7. No local de Criar Alerta de E-mail, no campo **Seu Endereço de E-mail**, digite seu endereço de e-mail se você deseja receber uma notificação por e-mail quando o relatório estiver processado.
8. Clique no botão **Continuar** para colocar o download em fila.
9. Quando sua solicitação for processada, recupere o arquivo CSV ou XML do relatório da página **Meus Relatórios**. Para mais informações, consulte "Baixando Relatórios" na página 150.

   O Relatório de Perfis de Chamadas baixado inclui os seguintes dados de cada dispositivo ativo:

   NOTA Para dispositivos Chrome, todas as horas de chamadas refletem a data e a hora em que as informações de dispositivos na Central do Cliente foram sincronizadas com as informações de dispositivos na sua conta do Google.

   - **ESN:** o Número de Série Eletrônico do dispositivo.
   - **Marca do Dispositivo:** o fabricante de um dispositivo ou outro hardware.

     NOTA Para todos os dispositivos Chrome, a marca é **Chromebook**.

   - **Modelo do Dispositivo:** o tipo de produto de um dispositivo ou outro hardware.
   - **Departamento:** o departamento a que este dispositivo pertence.
   - **Último Nome do Host**: o nome do servidor a partir de qual o agente realizou a chamada.
   - **Último Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo durante a última chamada de agente.
   - **Número de Série:** o número de série deste dispositivo.
   - **Número de Ativo:** o número de identificação associado a um dispositivo na Central do Cliente.
   - **Data de Ativação**: a data em que o agente contatou o Centro de Monitoramento a partir de um dispositivo pela primeira vez.
   - **ID do Último Chamador**: o endereço IP da origem da chamada recebida pelo agente ao Centro de Monitoramento.
   - **IP Local:** o endereço IP atribuído a um dispositivo na Rede Local (LAN) ao chamar o Centro de Monitoramento.
   - **Versão do Agente**: o número de versão do agente que contata o Centro de Monitoramento.
   - **Primeira Chamada**: a data e a hora da primeira chamada de agente ao Centro de Monitoramento.
   - **Última Chamada**: a data e a hora da chamada de agente mais recente ao Centro de Monitoramento.

- **Penúltima Chamada**: a data e a hora da penúltima chamada de agente ao Centro de Monitoramento.
- **Antepenúltima Chamada**: a data e a hora da antepenúltima chamada de agente ao Centro de Monitoramento.
- **Quarta Chamada a partir do Fim**: a data e a hora da quarta chamada de agente a partir do fim ao Centro de Monitoramento.
- **Quinta Chamada a partir do Fim:** a data e a hora da quinta chamada de agente a partir do fim ao Centro de Monitoramento.
- **Chamadas dos dias 0 a 30**: o número total de chamadas de agente ao Centro de Monitoramento nos últimos 30 dias.
- **Chamadas dos dias 31 a 60**: o número total de chamadas de agente ao Centro de Monitoramento nos últimos 31 a 60 dias.
- **Chamadas dos dias 61 a 90**: o número total de chamadas de agente ao Centro de Monitoramento nos últimos 61 a 90 dias.
- **Chamadas de há mais de 90 dias**: o número total de chamadas de agente ao Centro de Monitoramento de há mais de 90 dias.
- **Todas as Chamadas:** o número total de chamadas de agente ao Centro de Monitoramento.

Relatório de Auditoria do Usuário

O Relatório de Auditoria do Usuário permite que os administradores da Central do Cliente façam download de um arquivo CSV (valores separados por vírgulas) ou XML (eXtensible Markup Language) que identifica todos os usuários que foram adicionados ou modificados. O Relatório de Auditoria do Usuário não exibe dados na tela.

Para gerar um Relatório de Auditoria do Usuário:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Gerenciamento de Contas** > **Relatório de Auditoria do Usuário**.
3. No Relatório de Auditoria do Usuário, no campo **Nome**, digite um nome único para seu relatório.
4. No campo **Formato**, abra a lista e selecione uma das seguintes opções:
   - **CSV**: um arquivo de texto simples com colunas separadas por vírgula que é aberto com software incluído no seu sistema operacional. Recomendado para consultas SQL e o carregamento de arquivos de dados grandes.
   - **XML:** um arquivo de linguagem que é aberta com um editor de XML, tal como o Microsoft Excel ou OpenOffice. Recomendado para a filtragem e a formatação de dados.
5. No local de Criar Alerta de E-mail, no campo **Seu Endereço de E-mail**, digite seu endereço de e-mail se você deseja receber uma notificação por e-mail quando o relatório estiver processado.
6. Clique no botão **Continuar** para colocar o download em fila.
7. Quando sua solicitação for processada, você pode obter o arquivo CSV ou XML do relatório na página **Meus Relatórios**. Para mais informações, consulte "Baixando Relatórios" na página 150.

NOTA Enquanto a solicitação do arquivo está sendo processada, a coluna **Status** exibe **Em fila de espera** e o relatório não está disponível. Depois de processado, a coluna **Status** exibe o link **Pronto** e, se configurado para tal, a Central do Cliente envia uma notificação por email.

O Relatório de Auditoria do Usuário inclui os seguintes campos:

- **Alterado pela ID de Usuário**: o nome de usuário da Central do Cliente da pessoa que fez a alteração.
- **Alterado pelo Nome/Sobrenome de Usuário**: o nome da pessoa que fez a alteração.
- **Tipo**: a natureza da alteração. Os possíveis valores são **Inserir** (novo usuário criado), **Editar**, **Excluir**, ou **Reativar**.
- **Data/Hora da Alteração**: a data e hora quando a alteração foi feita.
- **Id do Novo Usuário**: o nome de usuário ou id de login novo ou alterado.
- **Novo E-mail**: o endereço de e-mail novo ou alterado associado ao usuário.
- **Novo Tipo de Usuário**: o valor modificado dos direitos de acesso do usuário, tal como ADMIN ou AVANÇADO.
- **Novo Nome/Sobrenome**: o nome e/ou sobrenome novo ou alterado associado à conta deste usuário.
- **Novo Grupo de Dispositivos**: o valor modificado do grupo de dispositivos.
- **Antiga ID de Usuário**: o antigo nome do usuário ou ID de login associado ao usuário.
- **Antigo E-mail**: os antigos endereços de e-mail associados à conta do usuário.
- **Antigo Tipo do Usuário**: os direitos de acesso associados ao antigo usuário, tal como ADMIN ou AVANÇADO.
- **Antigo Primeiro/Último Nome**: o primeiro e último nome associado à antiga conta de usuário.
- **Antigo Grupo de Dispositivos**: o grupo de dispositivos a que pertence a antiga conta de usuário.

Relatório de Eventos de Usuário

O relatório de Eventos do Usuário permite que os administradores da Central do Cliente visualizem um registro de usuários que foram suspensos da Central do Cliente ou que alteram suas senhas. A Central do Cliente registre o evento, a data e a hora da ocorrência, bem como o nome de usuário e o primeiro nome do indivíduo.

A Central do Cliente registra os seguintes tipos de eventos de usuário:

- Usuário reativado do estado de bloqueio temporário.
- Usuário permanentemente suspenso devido a falhas de login
- Usuário temporariamente suspenso devido a logins falhados
- Usuário permanentemente suspenso devido a inatividade
- Usuário permanentemente suspenso manualmente
- Usuário suspenso manualmente até a data especificada
- Usuário conectado/Senha validada
- Login do usuário falhou/Validação da senha falhou
- Senha Alterada
- Senha Redefinida
- Pergunta da senha alterada
- Usuário desconectado

- Usuário bloqueado manualmente
- Login rejeitado a endereço IP não autorizado

Para gerar um Relatório de Eventos de Usuário:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Relatórios** > **Gerenciamento de Contas** > **Relatório de Eventos de Usuário**.
3. No relatório de eventos do usuário, na área de **Pesquisar Critérios**, filtre os eventos que você deseja que seja retornados da seguinte forma:
   a) No campo **Nome de usuário contém**, digite todo ou parte do nome de usuário associado ao dispositivo.
   b) No campo **e o Detalhe do Evento contém**, digite um tipo de evento de usuário.
   c) Na área **e o Evento ocorreu**, faça uma das seguintes ações:
      - No campo **nos últimos <n> dias**, clique na opção e digite o número de dias desejado. Qualquer valor de **1** a **365** é apropriado. Um valor superior neste campo resulta em um relatório maior e demora mais tempo a ser gerado.
      - No campo **entre**, clique na opção e digite as datas (dd/mm/aaaa) ou clique no ícone do **Calendário** para abrir o diálogo do calendário. Digite as datas em ordem cronológica, com a data mais antiga introduzida primeiro e a mais recente introduzida depois.
4. Clique em **Mostrar resultados**, que atualiza a grelha de resultados e mostra os seguintes eventos de usuário com base na suas escolhas de filtragem.
   - **Para Nome de Usuário**: o nome de usuário da Central do Cliente associado ao evento de usuário
   - **Data e Hora**: a data e a hora em que o evento de usuário ocorreu
   - **Detalhes do Evento**: o tipo de evento de usuário que foi registrado
   - **Alterado por Usuário**: o nome de usuário do administrador que alterou uma senha. Quando o evento é acionado devido a inatividade ou tentativas de login falhadas, a coluna mostra **Sistema**.
   - **Alterado por Primeiro Nome**: o primeiro nome do administrador que alterou uma senha
   - **Alterado por Sobrenome**: o sobrenome do administrador que alterou a senha
   - **Endereço de IP Público**: O endereço IP público do dispositivo usado para se conectar à Central do Cliente

Meu Conteúdo

A área de relato de Meus Conteúdos na Central do Cliente é onde você armazena seus relatórios salvos e critérios de filtro. Os relatórios fornecidos na área **Meus Conteúdos** incluem:

- Meus Relatórios
- Meus Filtros

Meus Relatórios

Todos os relatórios da Central do Cliente podem ser baixados como arquivos CSV (Comma Separated Value) ou XML (eXtensible Markup Language). As solicitações de arquivos de relatórios são enfileiradas e processadas em offline. Quando o processamento estiver concluído, os arquivos CSV ou XML serão disponibilizados através da página Meus Relatórios.

A página Meus Relatórios mostra todos os downloads de relatórios solicitados e inclui as seguintes informações para cada relatório:

- **Relatório Solicitado Em**: mostra a data e a hora quando o arquivo CSV ou XML foi solicitado.
- **Nome de Relatório**: mostra o nome atribuído à solicitação do arquivo CSV ou XML.
- **Tipo de Relatório**: indica o tipo de relatório; por exemplo, **Importação de Grupo**.
- **Tamanho de arquivo**: mostra o tamanho do arquivo do relatório que você solicitou.
- **Status**: indica o status da solicitação, que pode ter os possíveis valores de **Em fila**, **Pronto** e **Erro**.

Para visualizar a página Meus Relatórios e baixar um relatório processado:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Meus Conteúdos** > **Meus Relatórios**.
3. Na página Relatórios, na linha contendo o relatório desejado, na coluna **Status**, clique no link **Pronto** e siga as instruções da tela para baixar o relatório.

NOTA Enquanto a solicitação do arquivo está sendo processada, a coluna **Status** exibe **Em fila de espera** e o relatório não está disponível. Quando processado, a coluna **Status** mostra o link **Pronto** e, se solicitado, a Central do Cliente envia uma notificação por email.

Meus Filtros

A página Meus Filtros mostra todos os filtros de relatórios salvos. Filtros salvos definem os critérios para um relatório, não o output de um relatório contido na grelha de resultados. Os dados que atendem a estes critérios podem mudar com o tempo, portanto o relatório de saída pode mudar também.

Para usar um filtro de relatório salvo:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Meus Conteúdos** > **Meus Filtros**.
3. Na página Meus Filtros, clique no nome de **Filtro** desejado na tabela.

O relatório é gerado novamente usando os critérios de filtro salvos.

Editando Filtros de Relatório Salvos

Para editar um filtro de relatório salvo:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Meus Conteúdos** > **Meus Filtros**.
3. Na página Meus Filtros, clique no nome de **Filtro** desejado na tabela.
4. O relatório é gerado novamente usando os critérios de filtro salvos.

Edite os filtros existentes e clique em **Mostrar Resultados**. O relatório é gerado novamente e é mostrado na página.

5. Se necessário, salve os filtros modificados como um novo filtro salvo. Para mais informações, consulte "Salvando Filtros de Relatório" na página 149.

NOTA O relatório original salvo permanece inalterado.

Capítulo 6: Usando a Tecnologia de Tempo Real

O recurso opcional da Tecnologia de Tempo Real (RTT) fornece comunicações em tempo real com dispositivos suportados, que é ativado usando um aplicativo Web que envia e recebe comunicações.

Se seu dispositivo estiver equipado com um adaptador de banda larga móvel suportado e atender aos requisitos mínimos do sistema, é possível usar o recurso de RTT para fazer o seguinte:

- Gerencie o equipamento móvel habilitado para banda larga na sua base de ativos.
- Forçar uma chamada de agente de um dispositivo usando mensagens SMS. Se o dispositivo gerenciado tiver uma conexão à Internet, ele contata o Centro de Monitoramento para receber instruções e tomar medidas imediatas.

O que é a Tecnologia de Tempo Real?

A Tecnologia de Tempo Real (RTT) permite que você rastreie melhor seus dispositivos equipados com a banda larga móvel. Adicionalmente, a RTT aproveita da banda-larga móvel e das mensagens SMS, também conhecidas por mensagens de texto, para aumentar consideravelmente o desempenho das funções de Rastreamento e Recuperação de Ativos do Computrace.

A RTT abrange os recursos seguintes:

- **Rastreamento de Adaptadores de Banda Larga Móvel (MBAT)**: O MBAT permite que os clientes do Computrace visualizem uma lista de adaptadores de banda larga móvel e seus atributos, incluindo informações acerca de equipamento, de assinantes e da rede na Central do Cliente. O MBAT é um recurso único que permite aos clientes do Computrace o rastreamento e gerenciamento de dispositivos através do uso de adaptadores de banda larga móvel e planos de dados nas suas bases de ativos.
- **Chamadas Iniciadas pelo Centro de Monitoramento (Monitoring Center-initiated Calling - MCIC)**: MCIC permite que os clientes iniciem remotamente uma chamada do agente Computrace usando a Central do Cliente. Chamadas Iniciadas pelo Centro de Monitoramento, em circunstâncias específicas, permitem uma redução drástica do tempo necessário para iniciar uma ação no dispositivo de destino. Por exemplo, as MCIC podem ser usadas para iniciar operações de Exclusão de Dados e de Congelamento de Dispositivos no dispositivo de destino, após apenas alguns minutos do envio de uma solicitação a partir da Central do Cliente. As MCIC também permitem o rastreamento e atualizações de geolocalização do ativo quase em tempo real. Na ausência das MCIC, cada uma dessas operações iniciarão apenas na próxima chamada agendada do Agente. Sob algumas circunstâncias, as MCIC também permitem a comunicação com computadores que não tenham uma conexão IP ativa.

Requisitos Mínimos do Sistema

Atualmente, as tecnologias RTT e MCIC não estão disponíveis para dispositivos com agentes para Macintosh, Linux, BlackBerry ou Windows Mobile. As tecnologias RTT e MCIC também não estão disponíveis para dispositivos de destino que estejam rodando o Absolute Manage.

Você necessita atender aos seguintes requisitos mínimos do sistema para usar o recurso de RTT:

- **Sistema Operacional**: O dispositivo de destino deve ter um dos sistemas operacionais do Windows suportados instalado nele. Consulte "Plataformas Suportadas para o Agente Computrace" na página 22.

- Dispositivos com base em Android necessitam de suporte para 3G
- **Processador:** O dispositivo de destino deve ter um dos seguintes processadores:
  - Intel Core i3
  - Intel Core i5
  - Intel Core i7
  - Intel Core i7 Extreme
- **Agente Computrace**: O dispositivo de destino deve ter um agente Computrace ativo instalado nele e dever fazer chamadas regulares para o Centro de Monitoramento da Absolute. Para informações sobre as versões mais recentes do agente, consulte "Baixando o Agente Computrace" na página 127.

  NOTA É altamente recomendado o uso do Agente Computrace versão 885 ou superior, pois tais dispositivos têm uma melhor taxa de sucesso de chamadas nas conexões de dados celulares.

- **Adaptador de Banda Larga**: O adaptador de banda larga móvel instalado no dispositivo de destino deve ser de um dos seguintes modelos ou uma variante próxima:
  - **Gobi**: 1000, 2000, 3000 e variantes
  - **Ericsson**: F3507g, F3607gw, e F5521gw
  - **Novatel**: Adaptadores de banda larga móvel sem-fios
  - **Sierra**: UMTS, MC5720 e MC 5725 Sem Fios

  Para uma lista completa de adaptadores de banda larga móvel suportados, consulte "Adaptadores de Banda Larga Móvel Suportados" na página 243.
- **Assinatura de Dados Válida Com Suporte a SMS**: O dispositivo de destino deve ter uma assinatura de dados móvel válida que suporte mensagens SMS.

IMPORTANTE Antes de usar a RTT, certifique-se de que o dispositivo de destino tem um agente ativo chamando regularmente para o Centro de Monitoramento da Absolute. Adicionalmente, você deve poder estabelecer uma conexão de dados e enviar e receber mensagens SMS usando o “aplicativo de vigilância” fornecido com o seu adaptador de banda larga móvel. Para mais informações, consulte as instruções fornecidas com seu adaptador de banda larga móvel ou com o dispositivo.

Adaptadores de Banda Larga Móvel Suportados

Os seguintes adaptadores de banda larga móvel são suportados:

- **Gobi 1000**: um adaptador de banda larga móvel integrado disponível nas redes UMTS e EVDO. Incluindo as seguintes variantes Gobi:
  - Qualcomm UNDP-1
  - Qualcomm 9202
  - Dell 5600
  - HP un2400
- **Gobi 2000**: um adaptador de banda larga móvel integrado disponível em redes UMTS e EVDO. Incluindo as seguintes variantes Gobi:
  - Qualcomm 920b
  - HP un2420

- **Gobi 3000**: um adaptador de banda larga móvel integrado apenas em dispositivos do Windows 7 e as redes UMTS e EVDO. Incluindo as seguintes variantes Gobi:
  - Sierra Wireless MC8355 (semelhante a HP un2430)
  - Dell DW5630 (pensa-se que é feito por Novatel Wireless), e,
  - Option GTM689W
- **Ericsson F3507g**: um adaptador de banda larga móvel UMTS integrado
- **Ericsson F3607gw**: um adaptador de banda larga móvel UMTS integrado
- **Ericsson F5521gw**: um adaptador de banda larga móvel UMTS integrado e as seguintes variantes apenas em dispositivos Windows 7:
  - Dell DW5550
  - HP hs2340
- **Adaptadores de banda larga móvel da Novatel Wireless** em redes UMTS e EVDO e Novatel Wireless E362 (semelhante a HP lt2510) somente no Windows 7
- **Adaptadores de banda larga móvel sem fios da marca Sierra**: adaptadores de banda larga móvel nas redes UMTS e CDMA/EVDO
  - Adaptadores de banda larga móvel UMTS da Sierra Wireless
  - Sierra Wireless MC5720: um adaptador de banda larga móvel CDMA/EVDO integrado
  - Sierra Wireless MC5725: um adaptador de banda larga móvel CDMA/EVDO integrado

NOTA Algumas variantes de marca OEM dos seguintes adaptadores de banda larga móveis podem ser suportados também.

Trabalhando com a RTT

Para receber e processar com sucesso os recursos de Tecnologia de Tempo Real (RTT) e de Chamadas Iniciadas pelo Centro de Monitoramento (MCIC), tais como mensagens SMS, o dispositivo de destino deve estar ligado e o adaptador de banda larga móvel no dispositivo deve estar:

- ligado
- associado a um serviço de SMS ativo
- dentro da área de cobertura da rede

Para mais informações sobre a pesquisa de dispositivos em sua conta com adaptadores de banda larga móvel, consulte "Relatório de Adaptador de Banda Larga Móvel" na página 166.

Para mais informações sobre os recursos de MCIC, tais como mensagens SMS, consulte os seguintes tópicos:

- "Visualizando o Registro de Chamadas Forçadas" na página 246
- "Iniciando uma Chamada Forçada" na página 247

Para aproveitar ao máximo das funcionalidades da RTT, seus dispositivos necessitam atender aos seguintes requisitos:

- Ative o recurso de RTT, incluindo o rastreamento de ativos de adaptadores de banda larga móvel e as Chamadas Iniciadas pelo Centro de Monitoramento, para sua conta ou para dispositivos individualmente gerenciados dentro da sua conta. Para ativar estes recursos, contate o Suporte Global da Absolute.

- Um dispositivo com suporte ao Computrace é um dispositivo que tem o agente Computrace instalado nele e que atende aos requisitos do Windows definidos anteriormente. Consulte "Requisitos Mínimos do Sistema" na página 242.
- Um adaptador de banda larga móvel suportado com um plano de dados ativo que tem suporte para SMS. Consulte "Adaptadores de Banda Larga Móvel Suportados" na página 243.

IMPORTANTE Somente Administradores de Segurança podem alterar as configurações de RTT na Central do Cliente. Administradores, Usuários de Segurança Avançados, Usuários Avançados e Usuários Convidados só podem ver e filtrar a lista de dispositivos RTT. Para mais informações, consulte "Funções de usuário e seus direitos de acesso" na página 96.

Esta seção inclui as seguintes tarefas:

- Visualizando Informações de Adaptadores de Banda Larga Móvel
- Editando o Número de Telefone Substituto
- Visualizando o Registro de Chamadas Forçadas
- Iniciando uma Chamada Forçada

Visualizando Informações de Adaptadores de Banda Larga Móvel

Para ver os detalhes do adaptador de banda larga móvel de um dispositivo habilitado com RTT:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Hardware** > **Relatório de Adaptadores de Banda Larga Móvel**.
3. Na página Relatório do Adaptador de Banda Larga Móvel, use o filtro para limitar sua pesquisa e clique em **Mostrar resultados**.
4. Na grelha de resultados, clique no link do **Identificador** do dispositivo que você deseja ver.
5. Na página de Resumo do Dispositivo, você verá os detalhes do dispositivo selecionado.

   Esta página abre com os conteúdos do separador do **Resumo do Hardware** aparecendo. Se você estiver usando um recurso de RTT, a quase a meio da página você verá a área dos **Adaptadores de Banda Larga Móvel**.
6. Clique no link de **Detalhes** para o dispositivo apropriado.

   O diálogo dos Detalhes do Adaptador de Banda Larga Móvel é aberto, fornecendo os seguintes detalhes sobre o dispositivo:

   - **Atributos de Hora Recolhidos**: a data e a hora quando as informações sobre o adaptador de banda larga móvel foram coletadas.
   - **Fabricante**: o nome do fabricante do adaptador de banda larga móvel.
   - **Modelo**: o número do modelo do adaptador de banda larga móvel, se disponível.
   - **ID do Equipamento**: o número de identificação único para o adaptador de banda larga móvel; geralmente disponível na parte inferior do notebook ou no adaptador de banda larga móvel. Para adaptadores EVDO, o Número de Série Eletrônico (ESN) e/ou o ID do Equipamento Móvel (MEID) podem ser relatados. Para redes UMTS, o Identificador Internacional de Equipamento Móvel (IMEI) é relatado.
   - **ID do Assinante**: o número único associado ao assinante; armazenado no adaptador, o chip Módulo de Identidade do Assinante (SIM) ou equivalente.

- **Rede**: a operadora de serviço móvel associada ao dispositivo móvel.
- **Status de Serviço**: o último status de disponibilidade relatado sobre a rede associada.
- **Número de Telefone Detectado**: o número de telefone associado ao adaptador de banda larga móvel, como relatado pelo dispositivo.
- **Número de Telefone Substituto**: o número de telefone alternativo ou substituto associado ao dispositivo móvel ou adaptador de banda larga móvel. Se o Computrace não detectar o número de telefone automaticamente, o dispositivo envia automaticamente um SMS para o Centro de Monitoramento. O endereço de "responder para" do SMS se torna no valor para o campo **Número de Telefone Substituto**. Você pode editar o número de telefone usando o diálogo **Editar Número de Telefone Substituto**. Consulte "Editando o Número de Telefone Substituto" na página 246.

7. No diálogo dos detalhes do adaptador de banda larga móvel, clique em **Fechar** para retornar à página do Resumo do Dispositivo.

Editando o Número de Telefone Substituto

O diálogo Editar Número de Telefone Substituto permite que você digite um novo número de telefone para usar no lugar do número de telefone detectado, ao enviar mensagens de texto SMS para o adaptador. As mensagens de texto SMS são usadas para contactar dispositivos, como parte do recurso de MCIC.

Para definir um número de telefone substituto:

1. Abra a página do Resumo do Dispositivo do dispositivo em que você deseja tentar uma chamada forçada ao completar a etapa 1 a etapa 5 da tarefa, "Visualizando Informações de Adaptadores de Banda Larga Móvel" na página 245.

   Para mais informações sobre a página do Resumo do Dispositivo, consulte "Editando Informações de Ativos" na página 141.

2. No separador **Resumo do Hardware**, na área **Adaptadores de Banda Larga Móvel**, para o adaptador desejado, clique no link **Editar** na coluna **Número Telefone Substituto**.
3. No diálogo **Editar Número de Telefone Substituto**, digite o novo número de telefone, incluindo os códigos de área e de país, no campo **Número de Telefone Substituto**. O número de telefone deve seguir o formato: +16045556789, sem espaços, parênteses, pontos ou hífens.
4. Clique em **Definir Substituto**.

   O diálogo de Editar Número de Telefone se fecha e a página Resumo do Dispositivo se atualiza e mostra o novo valor do número de telefone de substituição na coluna **Número de Telefone Substituto**.

Visualizando o Registro de Chamadas Forçadas

Na página do Resumo do Dispositivo, o separador de **Registros de Chamadas Forçadas** mostra informações detalhadas sobre os eventos associados a todas as chamadas forçadas realizadas em um dispositivo. O registro de chamadas forçadas mostra informações sobre mensagens SMS enviadas e recebidas do dispositivo. As seguintes informações estão disponíveis:

- **Hora**: a data e a hora associadas a um evento relacionado com chamadas forçadas.
- **Tipo**: a categoria do evento relacionado com a chamada forçada. Os possíveis eventos são: informação, aviso ou uma mensagem de erro.

- **Descrição**: os detalhes dos eventos que estão provocando a mensagem SMS ou a chamada forçada. Ao enviar uma mensagem SMS, a descrição inclui o número de telefone e o status inicial da operadora de serviço móvel.

  Ao receber uma resposta, a descrição inclui apenas o número de telefone.

Iniciando uma Chamada Forçada

Chamadas Iniciadas pelo Centro de Monitoramento (MCIC) , também conhecidas como chamadas forçadas, são mensagens SMS enviadas do Centro de Monitoramento para um dispositivo habilitado com a RTT, solicitando que o dispositivo inicie uma chamada de agente.

Para forçar uma chamada de um dispositivo:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Relatórios** > **Ativos de Hardware** > **Relatório de Adaptadores de Banda Larga Móvel**.
3. Na página Relatório do Adaptador de Banda Larga Móvel, use o filtro para limitar sua pesquisa e clique em **Mostrar resultados**.
4. Na grelha de resultados, clique no link **Identificador** para abrir a página do Resumo do Dispositivo para o dispositivo.
5. Siga as etapas apropriadas abaixo para forçar uma chamada para o dispositivo:
   - Para dispositivos com Windows:
     i) No separador **Resumo do Hardware**, na área **Adaptadores de Banda Larga Móvel**, na linha do adaptador desejado, clique em **Tentar Chamada Forçada**.
     ii) No diálogo Tentar Chamada Forçada, clique em **Tentar Chamada**.
     iii) O diálogo do Status de Chamadas Forçadas se abre, onde você verá o sucesso ou falha de sua solicitação.
        - O Centro de Monitoramento envia um SMS ao adaptador, solicitando uma chamada imediata do agente Computrace. Se o dispositivo está ligado e o adaptador de banda larga móvel está dentro da área de cobertura, o agente inicia uma chamada para o Centro de Monitoramento.
        - A mensagem é enfileirada se o adaptador de banda larga móvel não a conseguir receber.
        - Se o agente não tiver uma conexão à Internet, o agente contatará assim que estiver novamente online.

     iv) Clique em **Fechar**, que leva você de volta para a página do Resumo do Dispositivo para o dispositivo.
   - Para smartphones, no separador **Resumo do Hardware**, na área **Rádio de Smart Phone**, clique em **Tentar Chamada Forçada**.

     O Centro de Monitoramento envia uma mensagem SMS ao dispositivo móvel, solicitando uma chamada imediata do agente.

     Se o dispositivo está ligado e o adaptador de banda larga móvel está dentro da área de cobertura, o agente inicia uma chamada para o Centro de Monitoramento. Se não houver circunstâncias favoráveis, o agente chama quando todas as condições estiverem favoráveis e o dispositivo móvel estiver habilitado para receber a mensagem SMS e/ou iniciar uma chamada.

É possível visualizar o status de uma solicitação de uma chamada forçada no separador **Registros de Chamadas Forçadas**. Para mais informações, consulte "Visualizando o Registro de Chamadas Forçadas" na página 246.

É também possível forçar chamadas usando as MCIC como parte de solicitações de Exclusão de Dados e do Congelamento de Dispositivos. Para mais informações, consulte os seguintes tópicos:

- "Usando a Exclusão de Dados" na página 269
- "Usando o Congelamento de Dispositivo" na página 303

Capítulo 7: Usando a Tecnologia de Tempo Real sobre IP

Tecnologia de Tempo Real sobre IP (RTT-IP) reduz o tempo que demora para um administrador de conta a invocar operações remotas, tal como a Exclusão de Dados em dispositivos gerenciados do Windows e Mac. O uso de RTT-IP pode reduzir significativamente a janela de oportunidade para a perda de dados ou o acesso não autorizado a sistemas.

O recurso RTT-IP não está ligado por padrão e um administrador da Central do Cliente deve ativá-lo manualmente para sua conta.

Este capítulo fornece informações sobre os seguintes tópicos:

- Requisitos Mínimos do Sistema
- Compreendendo com a RTT-IP funciona
- Acelerando Operações com RTT-IP
- Ativando a RTT-IP
- Verificando que a RTT-IP funciona
- Editando o Período de Ping RTT-IP para um Dispositivo
- Visualizando os Status da RTT-IP para Todos os Dispositivos
- Pré-requisitos para a RTT-IP
- Desativando a RTT-IP

Requisitos Mínimos do Sistema

A RTT-IP funciona com dispositivos do Windows e Mac que atendam aos seguintes requisitos mínimos do sistema:

- Agente Windows versão 932 ou superior
- Agente Mac versão 934 ou superior
- Dispositivos que suportam os seguintes sistemas operacionais:
  - Mac OS X versão 10.5 ou superior
  - Windows 7 (qualquer edição)
  - Windows Vista (qualquer edição)
  - Windows 8 (qualquer edição)
- Acesso à Internet

Compreendendo com a RTT-IP funciona

Normalmente, quando você solicita uma operação de segurança, tais como a Exclusão de Dados ou o Congelamento de Dispositivos, em seus dispositivos na Central do Cliente, você necessita aguardar até a próxima chamada de agente agendada para a operação ocorrer. Por padrão, os dispositivos estão programados a fazer uma única chamada de agente a cada 24,5 horas. Portanto, você poderia esperar até este período de tempo para a operação de segurança ter efeito em seu dispositivo.

A RTT-IP reduz este tempo de espera em situações críticas em termos de tempo. O período de ping, que é independente do período de chamada do agente, é configurável. O recurso RTT-IP não está ligado por padrão e um administrador da Central do Cliente deve ativá-lo manualmente para sua conta. Para acomodar um retardamento de tempo mais curto, o agente Windows ou Mac em dispositivos habilitados com a RTT-IP realiza um ping leve, enviando 24 bytes de dados, sem incluir a largura de banda de cabeçalho HTTP. Este ping é enviado para um servidor de RTT-IP a um intervalo específico usando um canal separado daquele usado para chamadas de agente. Ativando a RTT-IP irá aumentar a carga na infra-estrutura de sua rede, incluindo em quaisquer servidores DNS, firewalls e proxies. Você deve coordenar com seu administrador de rede antes de ativar ou modificar suas configurações de RTT-IP. Particularmente, a ativação de RTT-IP em um grande número de dispositivos com períodos de ping elevados poderá ter um impacto adverso em sua rede. Para mais informações sobre a carga da infra-estrutura de rede adicional, consulte a Nota Técnica *TN130222 – A Carga da Infra/estrutura de Rede de RTT sobre IP* disponível na página Documentação da Central do Cliente.

Quando você ativa o recurso de RTT-IP em sua conta, pode selecionar o período de ping que é apropriado para sua empresa. O período de ping mais rápido que você pode definir usando a Central do Cliente para dispositivos em sua conta é de um ping a cada 15 minutos. Se você deseja adquirir períodos de ping mais rápidos de 1 a 15 minutos, entre em contato com o Suporte Global da Absolute Software. Para mais informações, consulte "Contatando o Suporte Global da Absolute Software" na página 23.

O recurso de RTT-IP é implementado de tal forma que quando você solicita uma operação de segurança, o agente é automaticamente instruído no próximo ping do dispositivo a realizar uma chamada de agente e, assim, iniciar a operação de segurança específica que você solicitou.

É possível forçar uma chamada quando quiser testar o recurso e validar que está funcionando em um dispositivo.

Pré-requisitos da RTT-IP

Clientes que pretendem usar a RTT-IP precisam de certificar que seus dispositivos atendam aos requisitos mínimos do sistema. Para mais informações, consulte "Requisitos Mínimos do Sistema" na página 249.

Acelerando Operações com RTT-IP

Para contas que estão configuradas para a RTT-IP, o recurso de RTT-IP interage com as operações de segurança da Central do Cliente e, portanto, requer usuários que estão familiarizados com o Computrace, preferencialmente administradores de rede ou membros da equipe de TI da sua empresa.

O recurso de RTT-IP é implementado de tal forma que quando você solicita uma operação de segurança, o agente é automaticamente instruído no próximo ping do dispositivo a realizar uma chamada de agente e, assim, iniciar a operação de segurança específica que você solicitou.

Este capacidade funciona com as seguintes operações de segurança:

- Solicitações de Exclusão de Dados
- Solicitações de Congelamento de Dispositivo e de Descongelamento de Dispositivos
- Solicitações de Lista Remota de Arquivos
- Solicitações de Recuperação Remota de Arquivos
- Envios de relatórios de furto

Monitorando o Status Online de Ativos

É possível usar o Relatório de Ativos para ver o status online de dispositivos com RTT-IP. O relatório de ativos mostra os seguintes indicadores de status para dispositivos:

Status	Descrição
	Indisponível: A funcionalidade de RTT-IP não está disponível para este dispositivo.
	Desativado: A RTT-IP não está ativada neste dispositivo.
	Online: RTT-IP está ativado neste dispositivo e uma conexão de rede está disponível. Pode forçar uma chamada a partir da página.
	Offline: RTT-IP está ativado, mas não existe uma conexão de rede disponível para este dispositivo.

Na página do Resumo do Dispositivo, a área de **RTT-IP** mostra a seguinte informação:

- O **Período de Ping** do dispositivo: Quando você liga o recurso RTT-IP em sua conta, deve selecionar um período de ping padrão. A não ser que você tenha especificado um período de ping diferente para este dispositivo, o valor neste campo corresponde aos padrões da conta.
- A **Hora do Último Ping** do dispositivo: Indica a última hora em que o dispositivo realizou um ping no servidor de RTT-IP.
- O status para o dispositivo: Quando o status for **Online**, você pode forçar uma chamada. É também possível forçar uma chamada quando o status for **Offline**, mas a solicitação permanece no status de **Enfileirada** até o dispositivo voltar a estar online.

Para mais informações sobre a página do Resumo do Dispositivo, consulte "Editando Informações de Ativos" na página 141.

Sua empresa pode escolher agrupar todos os dispositivos que estão habilitados com RTT-IP, caso em que você pode seguir as instruções fornecidas na tarefa, "Ativando a RTT-IP para Todos os Dispositivos em sua Conta" na página 251.

Ativando a RTT-IP

Há várias maneiras de ativar a RTT-IP para os dispositivos de sua empresa:

- Ativando a RTT-IP para Todos os Dispositivos em sua Conta
- Ativando a RTT-IP para um Dispositivo Individual

Ativando a RTT-IP para Todos os Dispositivos em sua Conta

Quando você usa a página Configurações da Conta para ativar a RTT-IP, você define um valor padrão que ativa este recurso em todos os dispositivos em sua conta.

Para ativar a RTT-IP para todos os dispositivos em sua conta:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Administração** > **Configurações da Conta**.

3. Na página Configurações da Conta, na lista **Configuração de RTT-IP - Período de Ping**, selecione o valor desejado.

   IMPORTANTE Ativando a RTT-IP aumenta a carga na infra-estrutura de sua rede, incluindo em quaisquer servidores DNS, firewalls e proxies. Coordene com seu administrador de rede antes de ativar ou modificar suas configurações de RTT-IP. Particularmente, a ativação de RTT-IP em um grande número de dispositivos com períodos de ping elevados poderá ter um impacto adverso em sua rede.

   Inicialmente, defina este intervalo para um período mais rápido ou para o que for mais apropriado para sua empresa. O período de ping mais rápido que você pode selecionar é um ping a cada 15 minutos. Se você deseja adquirir períodos de ping mais rápidos de 1 a 15 minutos, entre em contato com o Suporte Global da Absolute Software. Para mais informações, consulte "Contatando o Suporte Global da Absolute Software" na página 23.

4. Clique em **Salvar Alterações**.

5. No diálogo Aplicar Alterações, certifique-se de que a caixa de seleção **Todos os dispositivos** esteja selecionada e clique em **Continuar**.

   Para todos os dispositivos existentes na conta, a RTT-IP é ativada na próxima chamada de agente agendada a partir do dispositivo. Quando novos dispositivos são ativados na conta, a RTT-IP é ativada e o período de ping é aplicado

Ativando a RTT-IP para um Dispositivo Individual

É possível ativar a RTT-IP para dispositivos individuais em sua conta, usando a página Resumo do Dispositivo.

Para ativar a RTT-IP para um dispositivo individual:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Administração** > **Relatórios** > **Ativos de Hardware** > **Relatório de Ativos**.
3. Na página Relatório de Ativos, faça o seguinte:
   a) Na área **Critérios de Pesquisa**, no campo **o Grupo é** abra a lista e selecione **Todos Dispositivos**.
   b) Clique em **Mostrar resultados** e na grelha de resultados localize o dispositivo em que você deseja habilitar a RTT-IP.
   c) Clique no link de **Identificador** do dispositivo.
4. No Resumo do Dispositivo, marque a caixa de seleção **Ligar o recurso de RTT-IP para este identificador** para ativar RTT-IP para este dispositivo.
5. Defina o **Período de Ping da RTT-IP** para este dispositivo.

IMPORTANTE Ativando a RTT-IP irá aumentar a carga na infra-estrutura de sua rede, incluindo em quaisquer servidores DNS, firewalls e proxies. Coordene com seu administrador de rede antes de ativar ou modificar suas configurações de RTT-IP. Particularmente, a ativação de RTT-IP em um grande número de dispositivos com períodos de ping elevados poderá ter um impacto adverso em sua rede.

Inicialmente, defina este intervalo para um período mais rápido ou para o que for mais apropriado para sua empresa. O período de ping mais rápido que você pode selecionar é um ping a cada 15 minutos. Se você deseja adquirir períodos de ping mais rápidos de 1 a 15 minutos, entre em contato com o Suporte Global da Absolute Software. Para mais informações, consulte "Contatando o Suporte Global da Absolute Software" na página 23.

6. Clique em **Salvar Alterações**.

Verificando que a RTT-IP funciona

Verificando a funcionalidade de RTT-IP envolve o forçar de uma chamada e a verificação na Central do Cliente para ver se o dispositivo realizou uma chamada. Alternativamente, você pode executar um Congelamento de Dispositivo, que não é destrutivo para o dispositivo gerenciado.

Para verificar a funcionalidade da RTT-IP:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatórios** > **Relatórios de Hardware** > **Relatório de Ativos**.
3. Abra o relatório de ativos e na área **Critérios de Pesquisa**, no campo **o Grupo é**, abra a lista e selecione **RTT-IP**.
4. Clique em **Mostrar resultados** e na grelha de resultados você pode ver todos os dispositivos nesse grupo.
5. Clique no link do **Identificador** do dispositivo que você deseja que faça uma chamada.
6. Na página do Resumo do Dispositivo, na área de **RTT-IP**, faça uma das seguintes ações:
   - Se o status é **Online**, clique **Forçar uma chamada**.

     No diálogo do Status de Chamadas Forçadas, você será informado que o forçar da chamada foi inicializado com sucesso e que é esperado que o dispositivo faça uma chamada dentro do período de ping. Clique **Fechar**.
   - Se o status é **offline**, clique em **Forçar uma chamada** para enfileirar a chamada. Quando este dispositivo voltar a ficar online, a chamada é realizada e você recebe informações atualizadas.
7. Abra o Relatório de Ativos novamente e, para este dispositivo em particular, verifique a coluna de **Última Chamada** para ver a hora em que a chamada foi realizada.

Editando o Período de Ping de RTT-IP

Há duas maneiras de editar o período de ping da RTT-IP para os dispositivos de sua empresa:

- Editando o Período de Ping para os Dispositivos em Sua Conta
- Editando o Período de Ping RTT-IP para um Dispositivo

Editando o Período de Ping para os Dispositivos em Sua Conta

Se o período de ping atual definido a nível de conta não for satisfatório você pode alterá-lo. O novo período de ping pode ser aplicado a todos os dispositivos em sua conta ou a grupos seletos de dispositivos.

Para editar o período de ping da RTT-IP a nível de conta:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Administração** > **Configurações da Conta**.
3. Na página Configurações da Conta, na lista **Configuração de RTT-IP - Período de Ping**, selecione o valor desejado.
4. Clique em **Salvar Alterações**.
5. No diálogo Aplicar Alterações, faça uma das seguintes opções:
   - Para aplicar o período de ping em todos os dispositivos existentes e recém-ativados na conta, certifique-se de que a caixa de seleção **Todos os Dispositivos** esteja marcada.
   - Para aplicar as alterações a dispositivos específicos, desmarque a caixa de seleção **Todos os dispositivos** e selecione uma ou mais das seguintes opções:
     - **Definir o período de ping para novos dispositivos habilitados com a RTT-IP**: quando novos dispositivos são ativados na conta, a RTT-IP é ativada e o período de ping selecionado é aplicado.
     - **Ligue o recurso de RTT-IP para todos os dispositivos onde a RTT-IP está desligada**: ativa a RTT-IP e aplica o período de ping selecionado a dispositivos existentes.
     - **Alterar os dispositivos com um período de ping RTT-IP de** <valor atual> **para** <novo valor>: aplica o período de ping selecionado a dispositivos que estão habilitados com RTT-IP e os seus períodos de ping correspondem ao <valor atual>.
     - **Alterar os dispositivos que não possuem um período de ping RTT-IP de** <valor atual> **para** <novo valor>: aplica o período de ping selecionado a dispositivos que estão habilitados com RTT-IP e os seus períodos de ping não correspondem ao <valor atual>.
6. Clique em**Continuar**.

   O novo período de ping é aplicado quando o agente em cada dispositivo faz a próxima chamada de agente agendada para o Centro de Monitoramento.

Editando o Período de Ping RTT-IP para um Dispositivo

A configuração padrão para o período de ping de dispositivos é 30 minutos. É possível alterar esse período com base nas necessidades de sua empresa.

Para editar o período de ping para um dispositivo individual:

1. Conecte-se à Central do Cliente como um Administrador de Sistemas.
2. No painel de navegação, clique em **Administração** > **Relatórios** > **Ativos de Hardware** > **Relatório de Ativos**.
3. Na página Relatório de Ativos, faça o seguinte:

a) Na área **Critérios de Pesquisa**, no campo **o Grupo é** abra a lista e selecione **Todos Dispositivos**.

b) Clique em **Mostrar resultados** e na grelha de resultados localize o dispositivo em que você deseja habilitar a RTT-IP.

c) Clique no link de **Identificador** do dispositivo.

4. Na página Resumo do Dispositivo, na lista **Alterar Período de Ping RTT-IP**, selecione o valor desejado.

5. Clique em **Salvar Alterações**. O dispositivo recebe o novo período de ping quando o agente no dispositivo faz a próxima chamada de agente agendada ao Centro de Monitoramento. Chamadas de agente para o Centro de Monitoramento podem ocorrer uma vez em 24 horas.

Visualizando os Status da RTT-IP para Todos os Dispositivos

Se a RTT-IP estiver ativa para sua conta, você pode ver o status de RTT-IP de todos os dispositivos numa grelha de resultados.

Para ver o status da RTT-IP para todos os dispositivos:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Administração** > **Configurações da Conta**.
3. Na página Configurações da Conta, na área **Configuração RTT-IP**, sob **Status da RTT-IP**, clique no link **Ver**.

   NOTA O link de **Visualizar** está disponível apenas se um **Período de Ping** foi definido.

   No janela de Dispositivos que têm o recurso da RTT-IP ligado, as seguintes informações são exibidas para cada dispositivo:

   - Indicador do**status da RTT-IP** : indica o status da RTT-IP do dispositivo. Para visualizar a descrição do status, focalize o mouse sobre o indicador. Consulte "Monitorando o Status Online de Ativos" na página 251.
   - **Identificador**: o Identificador associado ao dispositivo. Clique neste link para abrir a página do Resumo do Dispositivo para o dispositivo.
   - **Nome de Usuário**: o nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo
   - **Sistema Operacional**: o software que controla a execução de programas de computador e de serviços no dispositivo.
   - **Versão do Agente**: o número de versão do agente instalado no dispositivo.
   - **Período de Ping**: o perído de tempo entre pings feitos pelo dispositivo para o servidor RTT-IP.
   - **Última Hora de Ping (UTC)**: a última hora em que o dispositivo realizou um ping no servidor de RTT-IP.

4. Para navegar, filtrar e ordenar os resultados, faça o seguinte:

   - Para alterar o número de registros exibidos em cada página da grelha de resultados, clique no campo **Por Página** e selecione uma opção da lista. As seguintes opções estão disponíveis:
     - 10

- 20
    - 50
    - 100
    - 500
    - 1000
- Para navegar para outra página nos resultados, clique no link da página aplicável (**<<Primeira**, **<Ant**, <N.º de página>, **Próx>** ou **Última>>**).
- Para fitrar os resultados, digite um valor para o Identificador, o Nome de Usuário, o Sistema Operacional, a Versão de Agente ou o Período de Ping no campo e clique em **Filtro**.

  NOTA Se você inserir apenas uma parte do valor, os resultados filtrados incluem todos os registros que satisfazem os critérios de filtragem. Por exemplo, se você digitar "win" para filtrar pelo sistema operacional Windows, todos os resultados que contêm "win", tal como o nome de usuário "Winston" serão incluídos nos resultados filtrados.

- Por padrão, os resultados são ordenados por Identificador. Para ordenar a informação por outros critérios, clique no cabeçalho de coluna desejado.

5. Ao concluir a revisão da informação, feche a janela.

Pré-requisitos para a RTT-IP

Os clientes necessitam garantir que os seguintes itens estão assegurados para aqueles dispositivos gerenciados em quais eles pretendem usar a RTT-IP:

- Atualize seu agente de PC do servidor para o seguinte:
    - Para dispositivos com Windows, o agente versão 920, que a Absolute faz automaticamente com uma lista de números de série eletrônicos (ESNs), também conhecidos como Identificadores.
    - Para dispositivos Mac, o agente versão 9xx.
- Dispositivos aplicáveis devem atender a todos os requisitos do sistema Consulte "Requisitos Mínimos do Sistema" na página 249.
- O número total de dispositivos que você deseja inscrever (começando com um quantidade de amostra).
- Infra-estrutura de rede, incluindo servidores proxy, gateways e assim por diante.
- Vontade de testar este recurso.
- Uma rede complexa com dispositivos que atravessam várias geolocalizações preferida quando se seleciona dispositivos para inscrever.

Desativando a RTT-IP

Há duas maneiras de desativar a RTT-IP para os dispositivos de sua empresa:

- Desativando a RTT-IP para Todos os Dispositivos em Sua Conta
- Desativando a RTT-IP em um dispositivo individual

Desativando a RTT-IP para Todos os Dispositivos em Sua Conta

Quando você usa a página Configurações da Conta para editar as configurações da RTT-IP, você define um valor padrão para este recurso para todos os dispositivos em sua conta.

Para desativar a RTT-IP para todos os dispositivos em sua conta:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Administração** > **Configurações da Conta**.
3. Na página Configurações da Conta, na lista **Configuração RTT-IP - Período de Ping**, clique em **Desligar RTT-IP**.
4. Clique em **Salvar Alterações**.

Desativando a RTT-IP em um dispositivo individual

É possível desativar a RTT-IP para dispositivos individuais em sua conta, usando a página do Resumo do Dispositivo.

Para desativar a RTT-IP para um dispositivo individual:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Administração** > **Relatórios** > **Ativos de Hardware** > **Relatório de Ativos**.
3. Na página Relatório de Ativos, faça o seguinte:
   a) Na área **Critérios de Pesquisa**, no campo **o Grupo é** abra a lista e clique em **Todos os Dispositivos**.
   b) Clique em **Mostrar resultados** e na grelha de resultados localize o dispositivo em que você deseja desativar a RTT-IP.
   c) Clique no link de **Identificador** do dispositivo.
4. Na página Resumo do Dispositivo, desmarque a caixa de seleção **Ligar o recurso de RTT-IP para este identificador** para desativar a RTT-IP para este dispositivo.
5. Clique em **Salvar Alterações**.

Capítulo 8: Protegendo seus dados e dispositivos

A Central do Cliente oferece as seguintes operações de segurança que habilitam os administradores de segurança e os usuários de segurança avançados a garantir que dispositivos gerenciados, e os dados que estes contêm, não sejam prejudicados em casos de perda ou furto:

- Exclusão de Dados (consulte "Usando a Exclusão de Dados" na página 269.)
- Congelamento do Dispositivo (consulte "Usando o Congelamento de Dispositivo" na página 303.)
- Intel® Anti-theft Technology (AT) (consulte "Concluindo o Suporte para a Intel Anti-Theft Tecnology" na página 266.)

  NOTA Somente os administradores de segurança podem executar operações de segurança da Intel® Anti-theft Technology.

- Lista de Arquivos (consulte "Usando a Lista de Arquivos" na página 339.)
- Recuperação Remota de Arquivos (consulte "Usando Recuperação Remota de Arquivos" na página 333.)

Para acessar estas operações de segurança, a Central do Cliente requer que Administradores de Segurança e Usuários de Segurança Avançados autorizados usem um código de autorização enviado por e-mail ou um código de um token RSA SecurID®. Sua empresa indica o método de autenticação que pretende usar quando você assina o Acordo de Administração de Segurança e Autorização de Geolocalização.

NOTA Usuários de segurança avançados podem executar operações de segurança em apenas aqueles dispositivos que pertencem ao grupo de dispositivos a que o usuário de segurança avançado foi atribuído.

Este capítulo inclui informações sobre os seguintes tópicos:

Antes de começar

Devido à natureza potencialmente destrutiva de alguns recursos de segurança, as seguintes verificações de segurança foram implementadas para garantir que as operações de segurança sejam iniciadas somente por pessoas autorizadas e que as operações de segurança sejam somente executadas nos dispositivos de destino corretos.

Certifique-se de que você atendeu aos seguintes pré-requisitos:

- A Absolute Software deve ter um acordo de pré-autorização assinado por sua empresa nos seus registros. Para mais informações, consulte "Acordo de Autorização de Administração de Segurança e da Geolocalização" na página 259. Este contrato é um pré-requisito para sua empresa receber uma conta da Central do Cliente. Sua conta indica à Central do Cliente que operações de segurança estão disponíveis para sua empresa.
- Para executar operações de segurança, tal como a Exclusão de Dados, você necessita de garantir que todos os seguintes pré-requisitos estão assegurados:

- ○ Um Nome de Usuário da Central do Cliente e uma Senha associadada que fornecem privilégios de autorização de segurança. Para mais informações, consulte "Funções de usuário e seus direitos de acesso" na página 96.
- ○ Um código de autorização gerado pelo seu token RSA SecurID® ou recebido da Central do Cliente em uma mensagem de e-mail, conforme o método de autenticação aplicável.

Cada operação de segurança deve ser fundamentada usando um código de autorização disponível apenas ao administrador de segurança ou usuário de segurança avançado que está solicitando o serviço de segurança. Para mais informações, consulte "Métodos de Autenticação de Segurança" na página 263.

- Os dispositivos de destino do serviço de segurança devem ter um agente ativado com um identificador único. Para mais informações, consulte "Baixando o Agente Computrace" na página 127.

NOTA Nenhum funcionário da Absolute Software, independentemente de seus direitos de acesso, pode iniciar uma operação de segurança para dispositivos em sua conta da Central do Cliente.

Acordo de Autorização de Administração de Segurança e da Geolocalização

Antes de você poder usar as operações de segurança disponíveis na Central do Cliente, a Absolute Software deve ter em seus registros um acordo de autorização assinado por sua empresa. O acordo de autorização identifica os funcionários em sua empresa autorizados a executar as operações de segurança e especifica o tipo de método de autenticação a ser usado pela empresa. O formulário de ativação de rastreamento por Geolocalização permite à Absolute Software saber se e como você está usando o recurso de rastreamento por Geolocalização.

Esta seção fornece as seguintes tarefas:

- Baixando e Enviando o Acordo de Autorização
- Desativando Acesso de Segurança para todos os Usuários de Segurança Autorizados
- Removendo Acesso de Segurança para um Administrador de Segurança Específico

Baixando e Enviando o Acordo de Autorização

Para baixar uma cópia em branco do acordo de autorização e enviá-la quando estiver concluída:

1. Conecte-se à Central do Cliente.
2. No painel de navegação ou nos links da parte superior da página, clique no link para **Documentação**.
3. Na área **Formulários de Solicitação de Serviço**, clique no link **Formulário de Autorização do Administrador de Segurança e da Geolocalização**.

   O acordo de autorização da administração de segurança e da geolocalização se abre em formato PDF.
4. Preencha os formulários do documento, imprima, assine, digitalize e anexe-o a um novo processo de suporte.
5. Para anexar o documento a um novo processo de suporte, faça o seguinte:

a) Clique no link do Suporte no painel de navegação ou nos links da parte superior da página para abrir a página do Suporte.

b) Na página Suporte, sob a área **Enviar um processo de suporte**, no campo **Tipo de problema**, abra a lista e clique em **Autorização do Administrador de Segurança e da Geolocalização**.

c) No campo **Título de problema**, digite um nome; por exemplo, **Autorização de Administradores de Segurança**.

d) No campo **Descrição do problema**, digite uma descrição; por exemplo, digite:

`Enviando nosso Acordo de Autorização de Administração de Segurança e da Geolocalização`

e) No campo **Severidade do problema**, abra a lista e selecione uma das seguintes opções:

- **1 – Crítico** indica que os processos de negócio críticos são gravemente afetados e está incluído um grande número de usuários.
- **2 – Urgente** indica que a empresa é afetada e está incluído um grande número de usuários; no entanto, os processos de negócio não estão afetados.
- **3 –Normal** indica que o negócio está moderadamente afetado, que a eficiência está impedida, mas os usuários podem ainda executar seu trabalho.
- **4 – Baixo** indica que o negócio não está afetado significativamente, embora o problema seja incomodativo. Este nível de severidade pode também indicar uma solicitação para uma melhoria.

f) Sob a área de **Anexo(s)** , em **Anexo 1:** clique em **Escolher Arquivo**, navegue para a localização da versão digitalizada de seu formulário preenchido e assinado, e clique em **Abrir** para anexá-lo.

g) Clique em **Enviar**.

O formulário é enviado para o Suporte Global da Absolute, onde os detalhes de sua conta são processados. Quando este processo for concluído, você recebe uma mensagem de e-mail de confirmação.

Desativando Acesso de Segurança para todos os Usuários de Segurança Autorizados

Caso você ache que a integridade de suas operações de segurança foi comprometida por qualquer razão, você pode desativar a autorização de segurança, que suspenderá o acesso de segurança de todo o pessoal autorizado.

AVISO! **Aja com cautela**. *A desativação da autorização do acesso de segurança suspende todos os administradores de segurança e usuários de segurança avançados, prevenindo que esses usuários façam solicitações de novas operações de segurança. Todas as solicitações de operações de segurança pendentes são processadas como habitualmente.*

Para habilitar o acesso a recursos que requerem a autorização de segurança novamente, você deve contatar Suporte Global da Absolute.

Para desabilitar o acesso de segurança de administradores de segurança à Central do Cliente:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Administração** > **Conta** > **Desativar Pré-Autorização**.

3. Na página Desativar Pré-Autorização, clique em **Desativar**.

IMPORTANTE Para ativar a autorização de segurança novamente, você deve contatar Suporte Global da Absolute. Para fazer tal, clique no link de **Suporte** e siga as instruções da tela.

Removendo Acesso de Segurança para um Administrador de Segurança Específico

NOTA Estas instruções aplicam-se tanto a administradores de segurança como usuários de segurança avançados. Para fins de explicação apenas, as informações nesta seção referem-se somente ao administrador de segurança.

Dependendo da sua situação, existem duas formas de remover o acesso de segurança de um administrador de segurança, ambas das quais estão descritas nesta seção como se segue:

- Removendo Acesso de Segurança ao Enviar um Caso de Suporte da Absolute Global
- Removendo Acesso de Segurança ao Suspender a Conta do Usuário

Removendo Acesso de Segurança ao Enviar um Caso de Suporte da Absolute Global

Se um determinado administrador de segurança deixar a sua empresa, ou mudar para uma outra função dentro dela, é possível instruir o Suporte Global da Absolute ao enviar um caso de suporte ou suspender a conta de usuário da Central do Cliente desse usuário, enquanto você notifica o Suporte Global da Absolute da alteração e criar uma autorização de segurança para um novo administrador de segurança.

Para remover o acesso de segurança de um administrador de segurança ao enviar um caso de Suporte Global da Absolute:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Suporte** > **Enviar um Caso de Suporte**, que irá abrir uma nova janela usada para contatar o Suporte Global da Absolute.
   a) No campo **Product**, abra a lista e selecione **Computrace** (página disponível apenas em inglês).
   b) No campo **Problem Type**, abra a lista e selecione **Account Administration** (página disponível apenas em inglês).
   c) Uma **Severity** de **3 - Standard** é apropriada para este tipo de solicitação (página disponível apenas em inglês).
   d) No **Title**, insira texto apropriado para este caso; por exemplo, **Removendo o Acesso de Segurança de <nome de usuário>**.
   e) No campo **Description**, dê indicações claras ao Suporte Global sobre aquilo que quer; por exemplo, Remova o acesso de segurança de <nome de usuário>, visto que a função de usuário desta pessoa foi alterada (página disponível apenas em inglês). Estamos enviando um novo formulário de Autorização do Administrador de Segurança e da Geolocalização para indicar o novo Administrador de Segurança.
   f) Digite as suas **informações de contato** e clique em **Save Case**.

   Na página de confirmação, você vê seu número do caso de suporte. Você poderá querer tomar nota do número, visto que será necessário no caso de contator o Suporte Global. Clique em **OK**, fecha esta janela e abra sua janela da Central do Cliente.

Quando o Suporte Global analisar seu caso de suporte e tomar ação, o acesso de segurança deste usuário é revocado e as operações de segurança já não estão dentro das capacidades deste usuário.

3. No painel de navegação da Central do Cliente, clique em **Documentação** e sob a área **Formulários de Solicitação de Serviço**, clique no link **Formulário de Autorização do Administrador de Segurança e da Geolocalização**.

   Siga as instruções neste formulário para indicar quais são os seus administradores de segurança (inclua tanto os antigos como os novos), complete este formulário na sua íntegra, incluindo a obtenção das assinaturas dos notadores e o envio deste acordo para o Suporte Global da Absolute.

Removendo Acesso de Segurança ao Suspender a Conta do Usuário

Suspendendo a conta da Central do Cliente do usuário previne que esse usuário registre quaisquer novas solicitações de operações de segurança, mas não afeta quaisquer solicitações pendentes. Por exemplo, se o administrador de segurança X tiver uma solicitação de uma Exclusão de Dados em aberto e sua conta da Central do Cliente for suspensa, a solicitação de uma Exclusão de Dados será executada como especificada na próxima chamada do agente. Para essas empresas que desejam limitar o acesso do usuário imediatamente, use as seguintes instruções.

Para remover o acesso de segurança de um administrador de segurança ao suspender os direitos desse usuário:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. Clique em **Administração** > **Usuário** > **Ver e Gerenciar Usuários**.
3. Na grelha de resultados, procure o administrador de segurança que deseja suspender na lista e clique no link **Editar** correspondente para abrir a página Criar e Editar Usuários dessa pessoa.
4. Sob a área **Configurações de status e suspensão de usuários** > **Status de Usuário**, clique na opção **Temporariamente suspenso até**, clique no calendário e selecione uma data de pelo menos 4 dias no futuro.

   NOTA Durante o intervalo de tempo que você selecionar, esta usuário particular não poderá conectar-se à Central do Cliente.

5. Clique em **Salvar**.
6. No painel de navegação, clique em **Documentação** e sob a área **Formulários de Solicitação de Serviço**, clique no link **Formulário de Autorização do Administrador de Segurança e da Geolocalização**.

   Siga as instruções neste formulário para indicar quais são os seus administradores de segurança (inclua tanto os antigos como os novos), complete este formulário na sua íntegra, incluindo a obtenção das assinaturas dos notadores e o envio deste acordo para o Suporte Global da Absolute.

   NOTA Pode demorar algum tempo para este formulário ter efeito. Se o usuário necessitar de acesso à Central do Cliente imediatamente, entre em contato com o Suporte Global da Absolute para obter assistência.

7. Dependendo de sua situação específica, faça uma das seguintes ações:

- Se este usuário vai deixar a sua empresa, siga as instruções na tarefa, "Excluindo Usuários" na página 115.
- Se este usuário vai ficar na sua empresa, siga as instruções na tarefa, "Ativando um usuário suspenso" na página 114.

Métodos de Autenticação de Segurança

A Absolute Software usa ou os tokens RSA SecurID® ou códigos de autorização únicos enviados por e-mail para substanciar as operações de segurança. Se você adquiriu a Central do Cliente diretamente da Absolute Software, você seleciona o Método de Autenticação de Segurança durante o preenchimento do acordo de autorização da Administração de Segurança e da Geolocalização. Se você adquiriu a Central do Cliente de um revendedor, pode especificar seu método de autenticação ao registrar sua conta em https://registration.absolute.com.

Esta seção oferece informações acerca dos seguintes tópicos:

- Usando Tokens RSA SecurID para Serviços de Segurança
- Usando Códigos de Autorização Enviados por E-mail para Serviços de Segurança
- Alterando Seu Método de Autenticação de Segurança

Usando Tokens RSA SecurID para Serviços de Segurança

Um token RSA SecurID® tem formato de chaveiro, é sincronizado com um servidor de banco de dados RSA da Absolute Software e gera um novo número aleatório de seis dígitos a cada sessenta (60) segundos. O token RSA SecurID é único e associado a uma conta individual de administrador de segurança ou de usuário de segurança avançado.

Se sua empresa está usando tokens RSA SecurID como método de autenticação, o administrador de segurança ou o usuário de segurança avançado digite o código do seu tokens RSA SecurID para validar cada operação de segurança.

RSA é a divisão de segurança da EMC^{2}®. No entanto, todos os tokens RSA SecurID devem ser adquiridos diretamente da Absolute Software.

Quando a Absolute Software receber o seu acordo de autorização assinado, nós enviamos os Tokens RSA SecurID® aos Administradores de Segurança e Usuários de Segurança Avançados autorizados por correio.

As seguintes informações e tarefas são fornecidas nesta seção:

- Usando Códigos de Tokens RSA SecurID
- Transferindo Tokens RSA SecurID

Usando Códigos de Tokens RSA SecurID

Contas que usam tokens RSA SecurID não precisam de solicitar um código de autorização de segurança. O token gera constantemente códigos de autorização de segurança. Quando o Administrador de Segurança ou o Usuário de Segurança Avançado solicitar uma operação de segurança, o código exibido no token é inserido no campo apropriado na página necessária, baseado na operação solicitada.

Um código do token SecurID é necessário para acessar operações de segurança para aquelas empresas que selecionam o método de autenticação de segurança dos tokens RSA SecurID. Quando você solicita uma operação de segurança, por exemplo, uma Exclusão de Dados, um Congelamento de Dispositivo, uma Recuperação Remota de Arquivos ou uma Remoção de Agente, a página Fornecer Autenticação será aberta. O administrador de segurança ou o usuário de segurança avançado depois insere sua senha da Central do Cliente e o código do token SecurID que aparece atualmente no token SecurID RSA.

Transferindo Tokens RSA SecurID

Quando um Administrador de Segurança ou um Usuário de Segurança Avançado muda de função ou sai da empresa, você pode transferir um Token RSA SecurID® existente para outro funcionário.

Para transferir um Token RSA SecurID:

1. Conecte-se à Central do Cliente.
2. Clique no link de **Documentação** no painel de navegação ou nos links da parte superior da página para abrir a página Documentação.
3. Na seção **Formulários de Solicitação de Serviços**, clique no link **Formulário de Transferência de Token RSA SecurID** para abrir o contrato de transferência de tokens em uma nova janela como um arquivo PDF.
4. Imprimir o contrato.
5. Preencha o formulário e o devolva por correio ou por fax para a Absolute Software, usando o endereço ou o número de fax fornecido no contrato.

Usando Códigos de Autorização Enviados por E-mail para Serviços de Segurança

Para empresas que selecionam códigos de autorização enviados por e-mail quando assinam o Acordo de Autorização de Administração de Segurança e da Geolocalização, um administrador de segurança ou um usuário de segurança avançado deve solicitar um códigos de autorização único através da Central do Cliente, antes de usar os serviços de segurança.

Um código de autorização de segurança é um identificador globalmente único (GUID) que é necessário para substanciar cada operação de segurança. Uma mensagem de e-mail, que inclui o código de autorização de segurança, é enviada para a conta de e-mail registrado para este usuário.

As seguintess condições se aplicam ao código de autorização de segurança:

- É válido por duas (2) horas a partir da hora de emissão para o destinatário apropriado.
- Apenas o usuário que solicitar o código de autorização de segurança pode usá-lo.
- O código de autorização de segurança só pode ser usado uma vez.

Esta seção fornece as seguintes informações para aquelas contas que optaram em ter códigos de autorização de segurança enviadas a endereços de e-mail específicos de Administradores de Segurança e de Usuários de Segurança Avançados:

- Solicitando um Código de Autorização de Segurança
- Alterando Endereços de E-mail para Pessoal de Segurança Autorizado

Solicitando um Código de Autorização de Segurança

Se sua empresa usa códigos de autorização enviados por e-mail para substanciar operações de segurança, você deve solicitar um código de autorização de segurança antes de iniciar qualquer ação na seção de Segurança de Dados e Dispositivos.

Quando receber o código de autorização de segurança, você usa-o para validar o serviço de segurança solicitado.

Para solicitar que um código de autorização de segurança seja fornecido em uma mensagem de e-mail:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos**> **Autorização de Segurança** > **Solicitar Código de Autorização**.
3. Na pagina Solicitar Código de Autorização, clique em **Solicitar Código**.

   A Central do Cliente mostra uma mensagem confirmando que um código de autorização foi gerado e o código de autorização de segurança foi enviado em uma mensagem de e-mail à conta de e-mail registrado para o Administrador de Segurança ou Usuário de Segurança Avançado que o solicitou.
4. A partir da mensagem de e-mail, copie o código de autorização de segurança para usar onde for apropriado.

Alterando Endereços de E-mail para Pessoal de Segurança Autorizado

Os administradores de segurança e os Usuários de Segurança Avançados podem alterar seus endereços de e-mail. Ao fazer isto, é importante saber que a Central do Cliente suspende temporariamente aqueles usuários de realizarem operações de segurança durante as próximas 72 horas. Para mais informações, consulte "Editando os Detalhes de um Usuário" na página 111.

Alterando Seu Método de Autenticação de Segurança

Não é possível alterar seu método de autenticação usando a Central do Cliente. Para alterar seu método de autenticação de segurança, entre em contato com o Suporte Global da Absolute Software em www.absolute.com/support.

Capítulo 9: Concluindo o Suporte para a Intel Anti-Theft Tecnology

Com a termininação da Intel® Anti-Theft Technology (Intel AT) no início de 2015, a Absolute concluiu o seu suporte do Intel AT na Central do Cliente. Todos os dispositivos equipados com Intel AT devem estar agora desinscritos do serviço na Central do Cliente.

Para detalhes da Intel sobre a terminação da Intel Anti-Theft Technology, consulte: www.intel.com/content/dam/www/public/us/en/documents/faqs/intel-anti-theft-service-faq.pdf.

Você pode continuar a proteger seus dispositivos do Windows gerenciados na Central do Cliente como se segue:

- Congele dispositivos usando o Congelamento de Dispositivos. Para mais informações, consulte "Solicitar um Congelamento de Dispositivo" na página 304.
- Estabeleça opções de bloqueamento de dispositivos e configurações de período do cronômetro semelhantes ao que estava disponível com o Intel AT usando as políticas de congelamento de dispositivos do estado offline. Para mais informações sobre estas políticas do estado offline e como criá-las, consulte "Gerenciando Políticas do Congelamento de Dispositivo do Estado Offline" na página 310.

Resolução de problemas de desinscrição do Intel AT

Se quaisquer dos seus dispositivos equipados com o Intel AT ainda estão ativos (Estado está definido para Intel AT Ligado), é provável que estes dispositivos ainda não tenham realizado chamadas para o Centro de Monitoramento durante algum tempo. Para resolver este problema você precisa desbloquear o dispositivo usando o token de recuperação do servidor. Em alguns casos, você poderá precisar instalar drivers do Intel AT atualizados se os drivers estiverem em falta ou desatualizados.

Dispositivos equipados com a Intel AT vêm pré-instalados com drivers da Intel AT, tais como:

- Driver de Interface de Controlador Embutido no Hospedeiro (HECI)
- Driver da Active Management Technology (AMT)
- Driver da Interface do Motor de Gerenciamento (MEI)

Esta seção oferece informações acerca dos seguintes tópicos:

- Visualizando o Status de Desinscrição de Dispositivos
- Desbloqueando Dispositivos Usando um Token de Recuperação de Servidor

Visualizando o Status de Desinscrição de Dispositivos

Para visualizar o status de seus dispositivos equipados com o Intel AT:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Intel® Anti-Theft Technology** > **Gerenciar dispositivos equipados com a Intel® Anti-Theft Tecnology**.

   A área do status da desinscrição do Intel® Anti-Theft Technology exibe as seguintes informações:

   - **Total de Dispositivos** inscritos no Intel AT.

- ○ **Dispositivos com o Intel AT desligado** indica o número de dispositivos que se desinscreveram do Intel AT . Você não precisa fazer nada com estes dispositivos.
- ○ **Dispositivos com o Intel AT ligado** indica o número de dispositivos que têm o Intel AT ligado.

3. Se quaisquer dispositivos ainda tiverem o Intel AT ligado, clique no link de **Ver** adjacente a **Dispositivos com o Intel AT ligado**.

   A grelha de resultados fornece detalhes para cada dispositivo. Consulte a coluna **Última Chamada** para ver quando foi a última chamada de cada dispositivo para o Centro de Monitoramento.

4. Se a coluna **Estado Atual** de um dispositivo mostrar **Bloqueado**, poderá ser possível desbloquear o dispositivo usando um token de recuperação de servidor. Para mais informações, .

   Depois do dispositivo ser desbloqueado, será desinscrito do Intel AT na próxima chamada de agente.

5. Caso haja algum erro da Intel AT prevenindo a desinscrição do dispositivo, um ícone ⚠ de aviso aparece na coluna **Estado Atual**. Focalize o mouse sobre o ícone para ver detalhes sobre o erro.

   - Para a lista de definições de códigos de erro, refira-se ao seguinte artigo da InTelligence Knowledge Base: KB-1076. Se o erro for relacionado com drivers do Intel AT em falta ou desatualizados, refira-se também ao seguinte artigo da InTelligence Knowledge Base: KB-1183.
   - Se necessitar de mais assistência, contate o Suporte Global. Consulte "Contatando o Suporte Global da Absolute Software" na página 23.

Desbloqueando Dispositivos Usando um Token de Recuperação de Servidor

Os administradores de sistemas podem usar um token de recuperação de servidor para desbloquear um dispositivo que foi bloqueado usando o Intel AT.

Esta seção inclui as seguintes tarefas:

- Gerando um Token de Recuperação de Servidor
- Usando um Token de Recuperação de Servidor para Desbloquear um Dispositivo Bloqueado

Gerando um Token de Recuperação de Servidor

Para gerar um token de recuperação de servidor para o seu dispositivo bloqueado:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Intel® Anti-Theft Technology** > **Gerenciar dispositivos equipados com a Intel® Anti-Theft Tecnology**.
3. Na página Gerenciar Dispositivos Equipados com a Intel® Anti-Theft Technology, procure pelo dispositivo apropriado bloqueado com Intel AT.
4. Na grelha de Resultados, clique em [ícone] na coluna **Identificador** do dispositivo apropriado.
5. No menu, clique em **Gerar Token de Recuperação de Servidor**.

6. Na página Gerar Tokens de Recuperação de Servidor, no campo **Digite ID da Plataforma de Recuperação**, digite o **ID da Plataforma de Recuperação** para o dispositivo bloqueado.

   NOTA A **ID de Recuperação da Plataforma** é exibida no dispositivo bloqueado.

7. Clique em **Gerar token de recuperação de servidor**.

   Se sua conta usa autenticação, a página Fornecer Autenticação se abre.

   a) Digite sua **Senha da Central do Cliente**.
   b) Digite seu **Código do Token SecurID** ou **Código de Autorização**.
   c) Clique em **OK**.

   A página Gerar Tokens de Recuperação de Servidor se atualiza e mostra o token de recuperação de servidor.

8. Registre o código para o Token de Recuperação de Servidor.

Usando um Token de Recuperação de Servidor para Desbloquear um Dispositivo Bloqueado

Para desbloquear um dispositivo bloqueado usando o token de recuperação do servidor:

1. Ligue o dispositivo bloqueado.
2. Na página Recuperação do Intel AT, especifique a opção de Token de Servidor (dependendo do dispositivo, você será instruído a digitar **2** ou **F2**).
3. Digite o token de reativação de recuperação de servidor usando a linha de números no teclado (e não o teclado numérico).
4. Pressione `Enter` para reinicializar seu dispositivo.

O dispositivo é desinscrito do Intel AT (estado do Intel AT definido como desligado) na próxima chamada de agente.

IMPORTANTE Se a desinscrição do dispositivo falhar, os drivers do Intel AT no dispositivo podem não estar presentes ou estão desatualizados. Para mais informações sobre como instalar novos drivers, refira-se ao seguinte artigo da InTelligence Knowledge Base: KB-1183.

Se necessitar de mais assistência com a resolução de problemas, contate o Suporte Global. Consulte "Contatando o Suporte Global da Absolute Software" na página 23.

Capítulo 10: Usando a Exclusão de Dados

A Exclusão de Dados permite que administradores de segurança e usuários de segurança avançados pré-autorizados da Central do Cliente excluam parte ou todos os dados do disco rígido de um dispositivo remoto. Usuários de segurança avançados podem executar uma operação de Exclusão de Dados em apenas aqueles dispositivos que pertencem ao grupo de dispositivos a que estes usuários foram atribuídos.

NOTA A Exclusão de Dados é disponibilizada somente com os serviços do Computrace®Plus, Computrace Complete, Computrace Data Protection, Computrace One, e ComputraceMobile.

Este capítulo inclui as seguintes seções:

Requisitos Mínimos do Sistema

A Exclusão de Dados está disponível para dispositivos que atendam aos seguintes requisitos mínimos do sistema:

- **Sistemas Operacionais**: O dispositivo de destino deve ter um dos sistemas operacionais suportados instalado Consulte "Plataformas Suportadas para o Agente Computrace" na página 22.

  NOTA A Exclusão de Dados não é suportado em dispositivos executando o sistema operacional Chrome OS.

- **Agente Computrace**: O dispositivo de destino deve ter um agente Computrace ativo instalado e chamando regularmente para o Centro de Monitoramento da Absolute. Para informações sobre as versões mais recentes do agente, consulte "Baixando o Agente Computrace" na página 127.

Algoritmos de Exclusão

O serviço de Exclusão de Dados usa diferentes algoritmos de exclusão para diferentes tipos de dispositivos e sistemas operacionais. O algoritmo usado em computadores com Windows excede em muito as recomendações documentadas pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos. Para obter detalhes adicionais, consulte *NIST Special Publication 800-88: Diretrizes para a Sanitização de Mídia: Recomendações da National Institute of Standards and Technology*, referenciadas em:nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

O algoritmo usado nos dispositivos Windows Mobile cumpre todos as diretrizes exceto a reposição do telefone para as definições de fábrica.

Em todos os sistemas operacionais, os dados não podem ser recuperados após a exclusão, mesmo com a utilização de software forense e ferramentas de análise de permanência de dados.

Os pré-requisitos para a Exclusão de Dados

A Exclusão de Dados pode não estar disponível para todos os dispositivos em sua conta, dependendo de outras operações de segurança em progresso, tais como o Congelamento de Dispositivo e a Recuperação Remota de Arquivos. O dispositivo em que você quer iniciar uma operação de Exclusão de Dados deve estar livre de conflitos com outras operações de segurança.

Antes de solicitar uma operação de Exclusão de Dados para um dispositivo, se aplicável, faça o seguinte:

1. Descongele o dispositivo se este tiver sido congelado por uma solicitação de congelamento de dispositivo ou uma política de congelamento de dispositivos do estado offline. Para mais informações, consulte "Descongelando um Dispositivo Congelado" na página 327.
2. Cancele quaisquer solicitações pendentes de Recuperação Remota de Arquivos ou aguarde que as solicitações sejam concluídas antes de solicitar a operação de Exclusão de Dados. Para mais informações, consulte "Cancelando uma Solicitação de Recuperação de Arquivo" na página 337.
3. Certifique-se de que qualquer Relatório de Furto associado está fechado, porque não é possível executar uma solicitação de Exclusão de Dados em um dispositivo com um Relatório de Furto aberto. Antes de executar uma operação de Exclusão de Dados, contate o Suporte Global da Absolute Software para fechar quaisquer Relatórios de Furto abertos associados ao dispositivo. Para informações sobre como entrar em contato com o Suporte Global da Absolute Software, consulte "Contatando o Suporte Global da Absolute Software" na página 23.
4. Certifique-se de que o Administrador de Segurança ou Usuário de Segurança Avançado que solicita a operação de Exclusão de Dados não alterou recentemente seu endereço de e-mail. Embora os endereços de e-mail possam ser alterados, fazendo isso suspende temporariamente aqueles usuários de realizarem operações de segurança durante as próximas 72 horas.
5. Se você estiver solicitando uma operação de Exclusão de Dados para fins de concessão ou de vida útil, desative quaisquer opções de segurança de dados e de dispositivos no dispositivo de destino antes de continuar. Falta de cumprimento pode resultar em múltiplas reinicializações do dispositivo de destino. Se estas pré-condições não forem cumpridas após cinco reinicializações e cinco chamadas bem-sucedidas do agente para o Centro de Monitoramento, a solicitação de Exclusão de Dados não se iniciará e o status se alterará para **Falhou**.

AVISO! Não é possível enviar uma solicitação de Exclusão de Dados de Fim da Concessão/Vida Útil para aqueles dispositivos com Criptografia de Discos Completos (FDE - Full Disk Encryption). O envio de uma solicitação de Exclusão de Dados de fim de contrato / vida útil para dispositivos com FDE pode causar que seu dispositivo pare de funcionar. Para enviar uma solicitação de Exclusão de Dados em tais casos, no campo **Motivo**, selecione **Outro** ou descriptografe o dispositivo antes de proceder com este tipo de solicitação de Exclusão de Dados.
Note também que para uma solicitação de uma Exclusão de Dados de Fim de Concessão/Vida Útil se concluir com sucesso, o dispositivo deve estar conectado à internet através de uma conexão de rede local(LAN). Se um dispositivo estiver usando uma conexão sem fios, sua solicitação de Exclusão de Dados permanece pendente.

Solicitando uma operação de Exclusão de Dados

As seguintes instruções assumem que você já assinou e entregou o Acordo de Autorização de Administração de Segurança e da Geolocalização da Absolute à Absolute Software e que já selecionou o seu método de autenticação de segurança. Consulte "Protegendo seus dados e dispositivos" na página 258.

IMPORTANTE Não é possível editar uma solicitação de Exclusão de Dados. No entanto, é possível cancelar uma solicitação, se a mesma não tiver sido iniciada no dispositivo destino. Para mais informações, consulte "Excluindo ou Cancelando uma Solicitação de Exclusão de Dados" na página 292. É também possível excluir uma solicitação se a solicitação estiver salva como um rascunho.

Esta seção fornece informações sobre os seguintes tópicos:

- Iniciando uma solicitação de Exclusão de Dados
- Registros de Exclusões
- Configurações de Exclusão de Dados

Iniciando uma solicitação de Exclusão de Dados

Para iniciar uma solicitação de Exclusão de Dados:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos**> **Exclusão de Dados** > **Solicitar Exclusão de Dados**.
3. Certifique-se de que tem atendido a todos os pré-requisitos. Consulte "Os pré-requisitos para a Exclusão de Dados" na página 270.
4. Se seu método de autenticação de segurança é o envio de códigos de autenticação de segurança por e-mail e você não solicitou nem recebeu um código de autorização para esta operação, na página Solicitar Exclusão de Dados, na área**Solicitar Código de Autorização**, clique em **Solicitar Código**.

   A Central do Cliente mostra uma mensagem confirmando que um código de autorização foi solicitado e enviado ao endereço de e-mail. Procure a mensagem no seu e-mail. Você precisará inserir o código na etapa 12 desta tarefa.
5. Na área de **Nome e Motivo da Solicitação de Exclusão de Dados**, faça o seguinte:
   a) No campo **Nome da Solicitação**, digite um nome apropriado para sua solicitação de Exclusão de Dados.
   b) No campo **Razão**, abra a lista e selecione um motivo a partir das seguintes opções:
      - Para dispositivos que estão perdidos, mas não furtados, clique em **Desaparecido**.
      - Se você quiser executar uma Exclusão de Dados por outros motivos, tal como preparar dispositivos para a reatribuição, clique em **Outro**.

- Para dispositivos que estão próximos do fim da concessão, da data de aposentação ou de serem tirados de serviço, clique em **Fim da concessão / vida útil**. Uma solicitação de Exclusão de Dados do Fim de Concessão/Vida Útil requer que o dispositivo seja reiniciado duas vezes antes da solicitação ser completada. Para garantir que uma solicitação de uma Exclusão de Dados seja completada com sucesso, desative o dispositivo na Central do Cliente antes de reinstalar o sistema operacional ou voltar a usar o dispositivo.

  IMPORTANTE Não é possível enviar uma solicitação de Exclusão de Dados de Fim da Concessão/Vida Útil para aqueles dispositivos com Criptografia de Discos Completos (FDE - Full Disk Encryption). O envio de uma solicitação de Exclusão de Dados de fim de contrato / vida útil para dispositivos com FDE pode causar que seu dispositivo pare de funcionar. Para enviar uma solicitação de Exclusão de Dados em tais casos, no campo **Motivo**, selecione **Outro** ou descriptografe o dispositivo antes de proceder com este tipo de solicitação de Exclusão de Dados.

  Note também que para uma solicitação de uma Exclusão de Dados de Fim de Concessão/Vida Útil se concluir com êxito, o dispositivo deve estar conectado à internet através de uma conexão de rede local (LAN). Se um dispositivo estiver usando uma conexão sem fios, sua solicitação de Exclusão de Dados permanece pendente.

6. Na área **Selecionar Dispositivos**, selecione um ou mais dispositivos de destino para sua operação de Exclusão de Dados, ao fazer o seguinte:

   a) Clique em **Selecionar Dispositivos** para abrir a caixa de diálogo Selecionar Dispositivos.

   b) No campo **Onde o grupo é**, abra a lista e selecione o grupo de dispositivos desejado.

   NOTA Se você estiver conectado como um usuário de segurança avançado, pode selecionar apenas o Grupo de Dispositivos a que está atribuído.

   c) Se você deseja mostrar dispositivos que cumprem critérios específicos, digite as informações apropriadas nos campos adjacente a **e o campo**.

   Por exemplo, você pode querer exibir apenas os dispositivos onde o campo **Nome de Usuário começa com** a palavra **Absolute**.

   d) Se você deseja incluir dispositivos para qual não poderá solicitar uma operação de Exclusão de Dados, selecione a caixa de seleção **Incluir Dispositivos Inelegíveis**.

   e) Clique em **Filtrar** para pesquisar na sua conta pelos dispositivos escolhidos e atualizar o diálogo Escolher Dispositivos para mostrar uma lista de dispositivos que correspondem aos seus critérios de sua pesquisa.

   f) Na lista de dispositivos, selecione as caixas de seleção adjacentes ao **Identificador** dos dispositivos nos quais você deseja executar a solicitação de Exclusão de Dados.

   IMPORTANTE Se você iniciar a Exclusão de Dados em um dispositivo com uma solicitação de Congelamento de Dispositivo no estado **Congelamento Solicitado**, a solicitação de Exclusão de Dados é implementada antes da solicitação de Congelamento de Dispositivo. O status da solicitação de Congelamento de Dispositivo é alterado para **Pendente** até que a Solicitação de Exclusão de Dados esteja concluída.

   g) Clique em **Continuar** para fechar o diálogo de Escolher Dispositivo e voltar à página de Solicitar a Exclusão de Dados.

Sob a área **Selecionar Dispositivos** você verá os dispositivos que selecionou.

7. Na área das **Configurações de Exclusão de Dados**, dependendo dos tipos de dispositivos que você selecionou, os separadores apropriados na seção de Configurações da Exclusão de Dados são ativados, da seguinte forma:

- Separador **PC** (número de dispositivos)

  i) No local **Selecione Tipo de Exclusão de Dados**, selecione uma das seguintes opções:

  - **Política Personalizada**
  - **Todos os Arquivos**
  - **Todos os Arquivos - Segurança**
  - **Todos os Arquivos, Limpeza de Setores e SO**

  NOTA Este definição não suporta discos rígidos SCSI.

  - **Erradicação de dados na Unidade de Firmware**

  Para mais informações sobre estas opções, consulte "Selecionando uma opção de tipo de Exclusão de Dados" na página 275.

  ii) Na local **Selecionar Opções da Exclusão de Dados**, faça uma das seguintes ações, se aplicável:

  - Abra a lista **Número de Sobrescrições de Dados** e selecione uma das seguintes opções:
  - Marque a caixa de seleção de **Exclusão Perpétua** para fazer com que a Exclusão de Dados se reinicialize no dispositivo de destino na próxima chamada de agente após o ciclo de exclusão se completar.
  - Marque a caixa de seleção de **Incluir Atributos de Datas de Arquivos** para incluir atributos de data de arquivos no arquivo de registro de exclusões.
  - Selecione a caixa de seleção de **Ignorar verificação de número de série do disco rígido** para permitir à Exclusão de Dados desprezar a verificação do Número de Série do Disco Rígido (HDSN - Hard Disk Serial Number).

  Para mais informações sobre estas opções, consulte "Selecionar Opções de Exclusão de Dados" na página 277.

- Separador **Mac** (número de dispositivos)

  Selecione uma das seguintes opções de **Selecionar Tipo de Exclusão de Dados**:

  - **Todos os Arquivos**
  - **Todos os Arquivos - Segurança**

  Para mais informações sobre estas opções, consulte "Configurações de Exclusão de Dados para Dispositivos Mac" na página 278.

- Separador **Dispositivos Móveis** (número de dispositivos)

  Selecione uma ou mais das seguintes opções:

  - **Excluir E-mails**
  - **Excluir Contactos**
  - **Excluir Registros de Telefone**
  - **Excluir Arquivos em Armazenamento Removível**
  - **Excluir Arquivos em Armazenamento Não Removível**

Para mais informações sobre estas opções, consulte "Configurações de Exclusão de Dados para Dispositivos Móveis" na página 279.

8. Se a solicitação de Exclusão de Dados se aplicar a um ou mais dispositivos habilitados com RTT, a caixa de seleção **Forçar uma chamada para dispositivos habilitados com MCIC** estará marcada por padrão na área **Chamadas Iniciadas pelo Centro de Monitoramento (MCIC)**. Para mais informações, consulte "Iniciando uma Chamada Forçada" na página 247.

   Depois do dispositivo de destino receber e processar a mensagem SMS, a solicitação de Exclusão de Dados é executada, dependendo das configurações de Exclusão de Dados especificadas para a conta.

9. Na área de **Comentários de Exclusão de Dados**, digite os comentários apropriados para esta solicitação de Exclusão de Dados no campo.

10. Na área **Validação de Exclusão de Dados**, faça o seguinte:

    a) Na área **Opção de E-mail Recebido**, se você desejar receber atualizações por e-mail sempre que o status da solicitação de Exclusão de Dados de qualquer dispositivo se altere, selecione a caixa de seleção **Eu aceito receber atualização por e-mail sobre o status de cada dispositivo**.

    NOTA Se a solicitação se aplicar a vários dispositivos, você pode receber numerosas mensagens de e-mail.

    b) Na área **Contrato de Exclusão de Dados**, leia a informação com atenção e selecione a caixa de seleção de **Eu aceito o contrato** para indicar que você leu o contrato e aceita os termos.

11. Clique em **Continuar** para atualizar a página Solicitar Exclusão de Dados, que mostra as informações de Exclusão de Dados específicas a esta solicitação.

12. Analise a informação e quando você estiver satisfeito que está tudo certo, clique em **Enviar Solicitação de Exclusão de Dados**, que irá atualizar a página Solicitação de Exclusão de Dados novamente para mostrar a área de **Fornecer Autenticação**. Faça uma das seguintes opções:

    - Se seu método de autenticação de segurança é códigos de autorização enviados por e-mail, digite sua **senha da Central do Cliente** e seu **Código de Autorização**.
    - Se seu método de Autenticação de segurança for tokens RSA SecurID, digite sua **senha da Central do Cliente** e seu **código de token SecurID**.

13. Clique em **OK**.

    Depois de iniciada, a operação de Exclusão de Dados é executada na próxima chamada do agente, mesmo se o usuário não fizer login no dispositivo.

    Quando o processo de Exclusão de Dados tiver começado, o mesmo não pode ser parado. Se a operação de Exclusão de Dados for interrompida por uma reinicialização do sistema, a Exclusão de Dados se reinicia apenas quando a tela de login do sistema operacional for exibida.

IMPORTANTE Em alguns casos, se a opção do número de série do disco rígido não estiver selecionada, a operação de Exclusão de Dados pode falhar porque o agente acredita que o dispositivo de destino é diferente do dispositivo selecionado. Se a operação de Exclusão de Dados falhar em tais casos, a Central do Cliente envia uma notificação por e-mail para o Administrador de Segurança ou ao Usuário de Segurança Avançado que solicitou a operação de Exclusão de Dados.

Registros de Exclusões

Quando a operação de Exclusão de Dados estiver concluída, você vai poder ver um arquivo de registro dentro da Central do Cliente. Este arquivo de registro exibe o nome da Solicitação de Exclusão de Dados e uma lista de todos os arquivos que foram excluídos. É possível examinar este arquivo de registro para confirmar que todos os dados sensíveis foram removidos, o que ajuda organizações a cumprir os regulamentos para operações de segurança. Para mais informações, consulte "Arquivos de Registro de Exclusão" na página 293.

IMPORTANTE Se você usa uma política de Exclusão de Dados que especifica **no boot without log file** (somente dispositivos com Windows), nenhum arquivo de registro estará disponível para visualização.

Configurações de Exclusão de Dados

Dependendo dos dispositivos que você selecionou para sua Solicitação de Exclusão de Dados, as opções no separador apropriado para cada tipo de dispositivo estarão ativas. Os três separadores seguintes estão disponíveis na seção de **Definições de Exclusão de Dados**:

- O separador **PC** permite que você especifique opções para dispositivos Windows. Para mais informações, consulte "Configurações de Exclusão de Dados para Dispositivos Windows" na página 275.
- O separador **Mac** permite que você selecione opções para dispositivos Mac. Para mais informações, "Configurações de Exclusão de Dados para Dispositivos Mac" na página 278.
- O separador **Dispositivos Móveis** permite a você especificar as opções para dispositivos móveis. Para mais informações, consulte "Configurações de Exclusão de Dados para Dispositivos Móveis" na página 279.

Configurações de Exclusão de Dados para Dispositivos Windows

O separador PC permite que você especifique definições detalhadas para seus dispositivos Windows. Esta seção fornece as duas seguintes tarefas:

- Selecionando uma opção de tipo de Exclusão de Dados
- Selecionar Opções de Exclusão de Dados

Dependendo das suas necessidades e as configurações do seu dispositivo, alguns ou todos os tipos de Exclusão de Dados e opções podem se aplicar à sua solicitação de Exclusão de Dados.

Selecionando uma opção de tipo de Exclusão de Dados

IMPORTANTE Siga com caução quando usar curingas. Por exemplo, digitar ***.s*** exclui todos os drivers do seu sistema, enquanto `*.d*` exclui todos os dlls, o que impossilita o restauro do sistema.

Selecione uma das seguintes opções de tipo de Exclusão de Dados:

- **Política Personalizada** é uma política previamente criada e salva que permite a você excluir arquivos e pastas específicos. O Sistema Operacional não será removido. O dispositivo continua a contactar o Centro de Monitoramento Absolute. Especifique a política personalizada de Exclusão de Dados usando um dos seguintes métodos:
  - Selecione o valor desejado da lista que aparece ao lado da opção de **Política Personalizada**.
  - Crie uma nova política para atender às suas necessidades específicas. Clique no link **Criar a Política**. A página Criar e Editar Políticas de Exclusão de Dados é aberta. Para instruções sobre como criar uma política de exclusão, consulte "Criando uma Política de Exclusão de Dados" na página 281.
- **Todos os arquivos** exclui todos os arquivos no dispositivo, incluindo arquivos recuperáveis. No entanto, o sistema operacional permanece. O dispositivo continua a contactar o Centro de Monitoramento. Quando a operação de exclusão for concluída, um arquivo de registros é enviado para o Centro de Monitoramento.

  Ao selecionar a opção de **Todos os Arquivos**, a pasta do Windows e a pasta raiz (geralmente `C:\`) não são excluídas. Todos os outros arquivos e pastas são excluídos. Adicionalmente, a Exclusão de Dados procura e exclui arquivos na pastas raiz e do Windows com as seguintes extensões:

.ACCDB	.ACCDE	.ACCDR	.ACCDT	.bak	.bmp	.csv	.doc
.docm	.docx	.dot	.dotm	.dotx	.gif	.htm	.html
.jpeg	.jpg	.mdb	.mpp	.msg	.ost	.pdf	.potm
.potx	.ppam	.ppsm	.ppsx	.ppt	.pptm	.pptx	.pst
.rtf	.tif	.tiff	.txt	.vsd	.xlam	.xls	.xlsb
.xlsm	.xlsx	.xltm	.xltx	.xml	.zip		

- **Todos os Arquivos - Segurança** exclui todos os arquivos no dispositivo de destino, incluindo arquivos recuperáveis. Todas as definições especiais e/ou componentes de software, tais como programas de Antivirus, software de criptografia, ou definições de proxy especiais, são excluídos, o que pode resultar ocasionalmente em uma reinicialização prematura ou em uma Exclusão de Dados incompleta. O dispositivo não pode inicializar o Windows até que o dispositivo seja formatado. Nós recomendamos a utilização da opção **Todos os Arquivos - Segurança** para dispositivos que foram relatados como perdidos ou furtados. Para melhores resultados, é recomendado que você crie uma política de exclusão personalizada que emula **Todos os Arquivos - Segurança** mas que deixa os arquivos necessários intatos para a conclusão do processo de Exclusão de Dados. Para instruções sobre como criar uma política de exclusão, consulte "Criando uma Política de Exclusão de Dados" na página 281.

  NOTA Limpeza de unidades e limpeza de setores não são suportadas em discos rígidos protegidos com Criptografia de Unidades BitLocker e Unidades de Criptografia Automática.

- **Todos os Arquivos, Limpeza de Setores e SO** remove todos os arquivos dos setores em todos os dispositivos de armazenagem de dados conectados, tal como discos rígidos internos e externos. O SO é removido também e o dispositivo pára de contatar o Centro de Monitoramento. Nós recomendamos a utilização do tipo **Todos os Arquivos, Limpeza de Setores e Exclusão de Dados do SO** para cenários de dispositivo em fim de concessão ou fim de vida útil. Se você quiser reatribuir a licença de produto da Absolute Software a um outro dispositivo, remova o agente do dispositivo que você está aposentando. Removendo o agente de um dispositivo liberta a licença e disponibiliza a mesma para um outro dispositivo. Para informações sobre como remover o agente de um dispositivo, consulte "Gerenciando solicitações de remoção de agentes" na página 132.

  NOTA Limpeza de unidades e limpeza de setores não são suportadas em discos rígidos protegidos com a Criptografia de Discos Completos (FDE - Full Disk Encryption). Solicitações de Exclusão de Dados de Fim de Contratos / Fim da Vida Útil não funcionam como esperado em disco rígidos configurados com RAID1. Discos Rígidos com RAID1 nunca mostram um status de **Concluído** no arquivo de Registos de Exclusão de Dados. Note também que para uma solicitação de uma Exclusão de Dados de Fim de Concessão/Vida Útil se concluir com sucesso, o dispositivo deve estar conectado à internet através de uma conexão de rede local(LAN). Se um dispositivo estiver usando uma conexão sem fios, sua solicitação de Exclusão de Dados permanece pendente.

- **Limpeza de Unidade Iniciada por Firmware**, também conhecida como uma Limpeza de BIOS Panasonic, está apenas disponível para unidades Panasonic pré-selecionadas. Selecione esta opção para excluir todos os dados de todos os discos rígidos internos. Quando a limpeza terminar, o SO e todos os dados no dispositivo serão removidos e, assim, o dispositivo já não conseguirá chamar para o Centro de Monitoramento. Para mais informações sobre centros de serviço, visite o site de Suporte da Panasonic em panasonic.net/support. A Limpeza de Unidades iniciada por Firmware não é furtivo.

  NOTA Limpeza de unidades e limpeza de setores não são suportadas em discos rígidos protegidos com Criptografia de Unidades BitLocker e Unidades de Criptografia Automática.

Selecionar Opções de Exclusão de Dados

Selecione uma ou mais das seguintes opções:

- **O Número de Sobrescrições de Dados** permite a você especificar quantas vezes a solicitação de Exclusão de Dados deve excluir os dados especificados e sobrescrever o mesmo com dados aleatórios ou de lixo para fazer com que a recuperação dos dados originais seja impossível. O processo de sobrescrição é chamado de “limpeza de dados”. Os possíveis valores da limpeza de dados são:
  - **1 Sobrescrita de Dados** — limpa os dados uma única vez. Este processo é o mais rápido e oferece o menor nível de segurança.
  - **3 Sobrescritas de Dados** — limpa os dados três vezes. Este processo é mais lento que o processo de 1 limpeza de dados e oferece um maior nível de segurança.
  - **7 Sobrescritas de Dados** é o valor padrão para a lista de **Número de sobrescrições de dados**. Este processo é o mais lento e oferece o maior nível de segurança.

- **A Exclusão Perpétua** reinicia a Exclusão de Dados no dispositivo de destino se o agente no dispositivo fizer uma chamada para o Centro de Monitoramento depois do ciclo de exclusão terminar. A opção de Exclusão Perpétua será desativada se você selecionar mais do que um dispositivo para sua solicitação de Exclusão de Dados.

  IMPORTANTE Selecionando uma Exclusão de Dados para um dispositivo que possui um relatório de furto aberto resultará no encerramento daquele relatório, visto que a Exclusão Perpétua removerá e/ou prevenirá a recolha de provas necessárias para recuperar o dispositivo.

- A opção **Incluir Atributos de data do Arquivo** inclui as datas de **Criação**, **Modificação**, e **Acesso** no arquivo de registro de Exclusão de Dados.

  Por padrão, somente as datas de **Criação** e de **Modificação** aparecem no arquivo de registro de dispositivos com Windows Vista e superior. Para incluir as datas de **Acessado**, você precisa também ativar as seguintes configurações nas Configurações de Conta: **Ativar carimbos de data/hora de último acesso de arquivo (apenas dispositivos do Windows)**. Para mais informações, consulte "Editando Configurações de Conta" na página 116.

  IMPORTANTE A inclusão dos atributos de data de arquivos aumenta o tamanho do arquivo de registro de Exclusão de Dados. Se o arquivo de registro for grande e o equipamento de destino tiver uma conexão de Internet com baixa largura de banda, a conclusão da Exclusão de Dados pode se atrasar enquanto o dispositivo cliente tentar repetidamente fazer o upload do arquivo de registro para a Central do Cliente.

- A opção **Ignorar verificação do número de série do disco rígido** permite a você especificar se a Exclusão de Dados deve desprezar a verificação do Número de Série do Disco Rígido (HDSN - Hard Disk Serial Number) e continuar mesmo quando o número de série do Disco Rígido for desconhecido ou se alterar durante o ciclo de vida da solicitação.

  IMPORTANTE Use o recurso de **Ignorar verificação de número de série do disco rígido** com cautela. A operação de Exclusão de Dados exclui dados no dispositivo de destino. Desprezando a verificação do HDSN antes de executar uma operação de Exclusão de Dados pode excluir dados criados por ou de propriedade de qualquer possessor pós-perda do dispositivo ou de uma disco rígido não relacionado.

  Se nenhum número de série de disco rígido é detectado no dispositivo de destino, a opção **Ignorar verificação do número de série do disco rígido** é selecionada por padrão. Para continuar, não altere o valor padrão.

Configurações de Exclusão de Dados para Dispositivos Mac

Selecione uma das seguintes opções:

- A opção **Todos os Arquivos Exceto SO** é idêntica à opção Excluir Todos os Arquivos Exceto SO para dispositivos Windows. Para mais informações, consulte "Configurações de Exclusão de Dados para Dispositivos Windows" na página 275.
- A opção **Todos os Arquivos Incluindo SO** é idêntica à opção Limpeza de Disco para dispositivos Windows. Para mais informações, consulte "Configurações de Exclusão de Dados para Dispositivos Windows" na página 275.

Configurações de Exclusão de Dados para Dispositivos Móveis

Selecione uma ou mais das seguintes opções:

- **Excluir E-mails** exclui todas as mensagens de e-mail baixadas para seu dispositivo móvel e todas as contas de e-mail configuradas no seu dispositivo. Dois itens a observar são:
  - Suas mensagens de e-mail não são excluídas de sua caixa no servidor do fornecedor de seu e-mail. É possível recuperar estas mensagens a partir de um outro dispositivo usando o website do seu fornecedor de e-mail.
  - Sua conta de e-mail nos servidores do fornecedor não será excluída.
- **Excluir Contatos** exclui todos os números de telefone e outras informações de seu dispositivo móvel.
- **Excluir Registros de Telefone** exclui informações acerca de todas as chamadas para e a partir de seu dispositivo móvel.
- **Excluir Arquivos em Armazenamento Móvel** remove todos os dados e arquivos armazenados em qualquer mídia de armazenamento de dados que você tem inserido no seu dispositivo móvel. Alguns exemplos de mídia de armazenamento de dados removível são cartões SD ou outros cartões de armazenamento.
- **Excluir arquivos em Armazenamento Não Removível** remove todos os dados e arquivos armazenados no seu dispositivo móvel.

Políticas de Exclusão

Para além das opções pré-definidas de Exclusão de Dados de *todos os arquivos exceto o sistema operacional* e *todos os arquivos incluindo o sistema operacional*, os Administradores de Segurança e Usuários de Segurança Avançados podem personalizar a Exclusão de Dados ao criar políticas de exclusão para excluir conjuntos específicos de arquivos e pastas.

Uma política de exclusão é uma lista criada pelo usuário com locais de arquivos e pastas. Quando a Exclusão de Dados é invocada, todos os arquivos no dispositivo de destino nos locais especificados são excluídos.

Esta seção fornece informações sobre os seguintes tópicos:

- Usando Amostras de Entradas de Arquivos de Política
- Excluindo uma Pasta Baseada numa Variável do Sistema do Windows
- Criando uma Política de Exclusão de Dados
- Editando uma Política de Exclusão
- Políticas de Exclusão

NOTA Políticas de Exclusão estão disponíveis somente para dispositivos com Windows.

Usando Amostras de Entradas de Arquivos de Política

Existem algumas entradas de arquivos de política úteis que você pode usar para criar uma política de exclusão:

- **no boot with log file**: Use esta entrada como a última entrada em um arquivo de política, somente aparecendo depois do processo excluir todos os outros arquivos específicos. Quando você selecionar esta entrada, a Exclusão de Dados carrega sempre o arquivo de registro daquilo que foi excluído para a Central do Cliente antes da limpeza de setores se iniciar.

- **no boot without log file**: Use esta entrada como a última entrada em um arquivo de política, somente aparecendo depois do processo excluir todos os outros arquivos específicos. Quando você seleciona esta entrada, a Exclusão de Dados inicia a limpeza de setores imediatamente depois de todos os arquivos especificados serem limpos. O agente não carrega um arquivo de registro para o Centro de Monitoramento nem o disponibiliza na Central do Cliente.
- **DELETE**: Anexe esta entrada a um caminho de registro para excluir qualquer chave (ou subchaves) do registro do Windows. Por exemplo, o arquivo de política seguinte exclui todas as subchaves existentes sob **Executar**:

  `DELETE_HKEY_LOCAL_MACHINE\SOFTWARE\Mcrosoft\Windows\CurrentVersion\Run`

  NOTA É possível excluir um arquivo ao referenciar sua chave de registro no registro do Windows. Por exemplo, `FILE_DELETE_HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\myapp` exclui o arquivo `C:\Program Files\myapp.exe`.

- **NO_DELETE**: Anexe esta entrada a um arquivo ou caminho de pastas para prevenir certos arquivos ou pastas de serem excluídos durante uma operação de Exclusão de Dados que normalmente iria excluir um grande conjunto de arquivos. Por exemplo, `C:\Project_Documents\NO_DELETE` certifica que uma operação de Exclusão de Dados não exclua a pasta de Project_Documents. Muitos produtos de criptografia usam um certo conjunto de arquivos para iniciar o dispositivo. Se uma operação de Exclusão de Dados forçar uma reinicialização, a fim de excluir arquivos bloqueados, o dispositivo não reiniciará com êxito se os arquivos necessários para o software de criptografia já tiverem sido excluídos. Isto impede que a operação de Exclusão de Dados termine, e o usuário não recebe uma confirmação da operação na Central do Cliente.
- **do not force reboot:** Use esta entrada para prevenir uma reinicialização quando uma operação de Exclusão de Dados encontrar arquivos bloqueados. Esta entrada é útil quando você está criando um arquivo de política em dispositivos com software de criptografia instalado, e forçando uma reinicialização pode fazer com que o dispositivo bloqueie porque alguns arquivos dos quais o software de criptografia necessita para iniciar o equipamento já foram excluídos. É possível usar a entrada **do not force reboot** em conjunto com a opção **NO_DELETE** para criar um arquivo de política que executa uma operação de Exclusão de Dados com sucesso em dispositivos com software de criptografia instalado.

Excluindo uma Pasta Baseada numa Variável do Sistema do Windows

É possível excluir uma pasta baseada numa variável do sistema do Windows ao especificar o nome da variável em um arquivo de política. O nome da variável deve ser delimitada com o carácter %. Por exemplo, a especificação **%windir%** exclui tudo na pasta de instalação do Windows, independentemente da localização física da pasta de instalação (i.e. unidade de disco C ou D). A Exclusão de Dados exclui todos os arquivos dentro da pasta e todas as suas subpastas, como especificado pela variável do sistema.

NOTA A Exclusão de Dados funciona apenas em variáveis de sistema. A operação de Exclusão de Dados não tem acesso às variáveis de usuário atuais. Além disso, quando uma nova variável do sistema for criada, a definição da variável não será carregada para a memória até à reinicialização do dispositivo. Portanto, a operação de Exclusão de Dados não é capaz de acessar a variáveis do sistema criadas dentro de uma dada sessão até à reinicialização do dispositivo.

Criando uma Política de Exclusão de Dados

Para criar uma Política de Exclusão de Dados:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Exclusão de Dados** > **Criar e Editar Políticas de Exclusão de Dados**.
3. Na página Criar e Editar Políticas de Exclusão de Dados, digite um nome para sua política de exclusão na caixa de texto **Nome da Política**.

   NOTA As políticas de Exclusão de Dados devem ter nomes únicos.

4. Digite uma breve descrição para sua política de exclusão na caixa de texto de **Descrição**.
5. Definir todos os arquivos e diretórios a serem excluídos. A Central do Cliente inclui diversas entradas predefinidas de diretórios e arquivos. Além disso, você pode definir suas próprias entradas únicas de arquivos e pastas. Uma única Política de Exclusão pode incluir qualquer combinação de entradas predefinidas e definidas pelo usuário.

   IMPORTANTE É também possível usar modelos de políticas para criar uma política de Exclusão de Dados. Para mais informações, consulte "Usando Modelos de Políticas de Exclusão de Dados" na página 283.

6. Para adicionar entradas pré-definidas:
   a) Clique em **Exclusões de Dados Pré-Definidas** para expandir a seção.
   b) Selecione as caixas de seleção para os tipos de arquivos que você deseja excluir.
7. Para definir e adicionar entradas únicas:
   a) Se não estiver já expandida, clique em **Exclusão de Dados Personalizadas**.
   b) No campo fornecido, digite uma entrada para cada arquivo ou pasta a ser excluída. Use a convenção padrão de caminhos de arquivos Windows e siga estas diretrizes:
      - O caractere curinga `*` é suportado, no entanto, nós recomendamos que você proceda com cautela quando o usa.
      - Ao especificar uma pasta, certifique-se de incluir uma barra invertida delimitadora após o nome da pasta; por exemplo, `c:\temp\`. Todos os arquivos da pasta principal e todos os arquivos e subpastas serão excluídos. O diretório raiz vazio é retido.
      - Para excluir uma pasta, inclua uma barra invertida no fim do caminho, por exemplo: `c:\pasta\`.
      - Para excluir um arquivo, não inclua uma barra invertida no fim do caminho, por exemplo: `c:\folder\xyz.doc`

A seguinte tabela fornece mais exemplos.

Para excluir...	digite isto:
uma pasta na unidade C	`c:\pasta\`
uma pasta específica em todas as unidades	`*:\pasta`
um tipo de arquivo específico em uma pasta específica na unidade C	`c:\pasta\*.abc`
um arquivo específico em uma pasta específica na unidade C	`c:\pasta\arquivo.abc`
uma variável específica no registro	`%variavel_meu_ambiente%`
todos os arquivos para um tipo de arquivo específico	`*.abc`

8. Para especificar entradas de chave do registro ou tipos de arquivos específicos:
   a) Clique em **Exclusão de Dados do Registro** para expandir a seção.
   b) Para excluir uma entrada de chave do registro e todas as subchaves sob a chave:
      i) Na lista **Tipo de Exclusão de Registro e Valor de Entrada Chave**, selecione **Exclui chave em**.
      ii) No campo **Tipo de Exclusão de Registro e Valor de Entrada de Chave**, digite a chave em um formato de chave de registro apropriado. Por exemplo, para excluir a chave e todas as subchaves, adicione:
      `HKEY_LOCAL_MACHINE\SOFTWARE\MyKey`
      iii) Clique em **Adicionar** para adicionar a entrada.
   c) Repita Etapa b para adicionar todas as chaves e subchaves que você deseja excluir.
   d) Para excluir um arquivo localizado sob uma chave do registro específica:
      i) Na lista **Tipo de Exclusão de Registro e Valor de Entrada de Chave**, selecione **Excluir ARQUIVO localizado em**.
      ii) No campo **Tipo de Exclusão de Registro e Valor de Entrada de Chave**, digite a chave que contém o caminho físico para o arquivo que deseja excluir. Por exemplo, para excluir o arquivo `C:\Program Files\app_name.exe`, que se encontra sob a chave de software de MyApp, adicione:
      `HKEY_LOCAL_MACHINE\SOFTWARE\MyApp`
      iii) Clique em **Adicionar** para adicionar a entrada.
   e) Repita Etapa d para adicionar todos os arquivos de uma chave de registro que você deseja excluir.
9. Para reter os dados em pastas específicas ou para arquivos e tipos de arquivos específicos: arquivos e pastas específicos:
   a) Clique em **arquivos ou pastas Excluídos** para expandir a seção.
   b) Adicione a lista de arquivos e pastas que você deseja excluir da operação de Exclusão de Dados no mesmo formato que usou para a Exclusão de Dados Personalizada.
   c) Se você quiser forçar uma operação de Exclusão de Dados em arquivos ou pastas que se encontram na lista de arquivos e pastas excluídos que você especificou na etapa anterior, clique em **Para forçar uma operação de Exclusão de Dados em arquivos e pastas localizadas na lista acima**.
   d) Adicione a lista de arquivos e pastas no campo fornecido.

NOTA Para mais informações sobre o formato dos comandos usados, consulte "Criando uma Política de Exclusão de Dados" na página 281.

10. Para especificar outras opções:
    a) Se não estiver já expandida, clique em **Opções**.
    b) Se quiser executar exclusões adicionais, selecione **Executar exclusões adicionais**.
    c) Selecione uma das seguintes opções:
       - **Erradicar arquivos recuperáveis**: Esta opção exclui de forma segura quaisquer arquivos excluídos anteriormente que sejam recuperáveis.
       - **Limpar espaço livre**: Esta opção exclui de forma segura quaisquer dados que permaneçam no espaço do disco usado.
    d) Se quiser tornar o dispositivo de destino incapaz de ser inicializado, selecione **Tornar dispositivo de destino incapaz de ser inicializado**.
    e) Selecione uma das seguintes opções:
       - **Imediatamente após a operação de Exclusão de Dados ser concluída**: Esta opção não fornece qualquer arquivo de registro.
       - **Após o arquivo de registros ser carregado**: Esta opção impede o dispositivo de inicializar para o sistema operacional depois do arquivo de registro da Exclusão ser carregado para a Central do Cliente.
    f) Se você não quiser forçar uma reinicialização do dispositivo que tem arquivos abertos ou bloqueados, ou a criptografia de discos completos ativa, selecione a opção **Não forçar reinicialização se o dispositivo de destino tiver arquivos bloqueados ou criptografia de discos completos ativa**. Em tais casos, a operação de Exclusão de Dados pausa até que o dispositivo seja reinicializado.
11. Quando você tiver configurado todas as descrições desejadas, clique em **Salvar**.

Usando Modelos de Políticas de Exclusão de Dados

A Central do Cliente fornece modelos de políticas que contêm amostras de texto e exemplos para cenários de Exclusão de Dados selecionados. É possível usar modelos de políticas para criar políticas de Exclusão de Dados muito mais rápido ao copiar e colar os textos desejados.

Os seguintes cenários de amostra da Exclusão de Dados estão disponíveis:

- Eu tenho Criptografia de Disco Completo CheckPoint.
- Eu quero excluir primeiro os arquivos confidenciais e depois desativar o Cisco VPN no dispositivo.
- Depois das pastas dos perfis de usuário do Windows serem excluídos, eu apenas necessito tornar o dispositivo inarrancável o mais depressa possível.

Para usar Modelos de Políticas de Exclusão de Dados:

1. Na página Criar e Editar Políticas de Exclusão de Dados, clique em **Ver Modelos de Políticas**. A janela dos Modelos de Políticas aparece.

   NOTA É possível redimensionar e mover a janela.

2. Clique no cenário desejado para fazer expandi-lo.

3. Copie e cole o texto de amostra em cada campo desejado na seção correspondente.
4. Na seção de **Opções** na página Criar e Editar Políticas de Exclusão de Dados, selecione as mesmas opções que vê no **Exemplo**.
5. Clique **Fechar**.

Editando uma Política de Exclusão

O processo de editar uma Política de Exclusão é semelhante ao processo de criar uma Política. As políticas de exclusão só podem ser editadas por Administradores de Segurança e Usuários de Segurança Avançados autorizados.

NOTA Não é possível modificar uma Política de Exclusão se estiver associada a uma solicitação ativa de Exclusão de Dados.

Para editar uma Política de Exclusão:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos**> **Exclusão de Dados** > **Ver e Gerenciar Políticas de Exclusão de Dados**. A página Visualizar Políticas de Exclusão de Dados abre, mostrando todas as Políticas de Exclusão definidas atualmente.
3. Clique no link **visualizar** da política de exclusão que você deseja modificar. A página Criar e Editar Políticas de Exclusão de Dados se abre e mostra a configuração atual da Política de Exclusão selecionada.
4. Caso deseje alterar o nome da política, digite o novo nome na caixa de texto de**Nome da Política**.

   NOTA As Políticas de Exclusão de Dados devem ter nomes únicos.

5. Faça as alterações desejadas na política de exclusão e depois clique em **Salvar**

Rastreamento de Status de Exclusão de Dados

A Central do Cliente fornece atualizações de status em tempo real sobre o progresso das solicitações de Exclusão de Dados. Adicionalmente, ao completar com sucesso uma operação de Exclusão de Dados, a Central do Cliente armazena um registro de exclusões que mostra todos os arquivos e pastas que foram excluídos.

Visualizando o Status de Exclusão de Dados

Para visualizar o status de uma solicitação de Exclusão de Dados:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Exclusão de Dados** > **Relatório do Resumo de Exclusão de Dados**.

3. Na página Relatório de Resumos de Exclusão de Dados, na área **Critérios de Pesquisa**, defina as opções de filtragem e de exibição preferidas para os resultados, usando um ou mais dos seguintes critérios:

   - Para filtrar os resultados por grupos de dispositivos, no campo **Onde o grupo é**, abra a lista e selecione o grupo de dispositivos desejado.

     NOTA Se você estiver conectado como um usuário de segurança avançado, pode selecionar apenas o Grupo de Dispositivos a que está atribuído.

   - Para filtrar os resultados por **Identificador**, **Marca**, **Modelo**, ou **Número de Série** específico, abre a lista e selecione o tipo de valor no campo **e no campo**.

     No campo **é ou contém** digite o valor para ser pesquisado ou use o recurso **Escolher**. Para mais informações sobre o recurso **Escolher**, .consulte "Editando Informações de Ativos" na página 141.
   - Para filtrar por nome de solicitação, no campo **e o Nome de Solicitação é ou contém**, digite um nome parcial ou o nome completo da solicitação de Exclusão de Dados.
   - Para filtrar por status, na área **e o status de Exclusão de Dados é**, selecione uma ou mais caixas de seleção a partir destes possíveis valores:
     - **Solicitada**: A solicitação foi submetida e está em estado transitório enquanto as instruções da Exclusão de Dados são configuradas. As solicitações de Exclusão de Dados ficam neste estado de forma breve.
     - **Executada**: As instruções da Exclusão de Dados foram enviadas para o dispositivo de destino e esse dispositivo já fez uma chamada e recebeu as instruções da solicitação da Exclusão de Dados.
     - **Acionada**: Somente para a limpeza de BIOS Panasonic, este estado é semelhante ao de Executada, mas é um estado final. A limpeza de BIOS Panasonic não devolve um estado de **Falhou** ou **Concluída** para as solicitações de Exclusão de Dados.
     - **Cancelada**: A solicitação de uma Exclusão de Dados foi cancelada.
     - **Limpa**: O dispositivo de destino foi recuperado antes da operação de Exclusão de Dados começar. A equipe de Investigações da Absolute cancelou a solicitação.
     - **Definida, aguardando chamada**: O Centro de Monitoramento está configurado para enviar as instruções de Exclusão de Dados para o dispositivo de destino na sua próxima chamada.
     - **Concluída, Tentando carregar o Arquivo de Registro (Se Aplicável)**: A Exclusão de Dados foi concluída no dispositivo de destino, no entanto, o agente não foi capaz de enviar o arquivo de registro para o Centro de Monitoramento. Se especificado para a sua conta ou o dispositivo, o agente continua a iniciar chamadas para o Centro de Monitoramento até que o arquivo de registro seja carregado para o mesmo.
     - **Concluída, Arquivo de Registro Carregado**: A Exclusão de Dados foi concluída no dispositivo alvo e o agente enviou um arquivo de registro com detalhes da operação de Exclusão de Dados para o Centro de Monitoramento.
     - **Falhou**: A solicitação de Exclusão de Dados falhou em ser executada no dispositivo de destino. Entre em contato com o Suporte ao Cliente. Consulte "Contatando o Suporte Global da Absolute Software" na página 23.
     - **Processando**: A Central do Cliente esta criando a solicitação de Exclusão de Dados. As solicitações de Exclusão de Dados passam pelo estado de processamento antes de entrarem no estado de Solicitada.

- Para filtrar por opções de Exclusão de Dados, na área de **e o tipo de Exclusão de Dados é** , selecione uma ou mais caixas de seleção a partir das seguintes escolhas possíveis:
  - **Política Personalizada**: a operação exclui arquivos e pastas específicos.
  - **Todos os Arquivos**: a operação exclui todos os arquivos, exceto o Sistema Operacional.
  - **Todos os Arquivos - Segurança**: a operação exclui todos os arquivos, incluindo o Sistema Operacional e, depois da conclusão da primeira operação de Exclusão de Dados, limpa os discos rígidos conectados. A solicitação de Exclusão de Dados é acionada por uma violação de segurança e a necessidade de remover dados confidenciais de um dispositivo.
  - **Todos os Arquivos, Limpeza de Setores e SO**: a operação exclui todos os arquivos incluindo o Sistema Operacional e limpa o disco rígido após a conclusão da solicitação. A solicitação de Exclusão de Dados é acionada pela necessidade de aposentar o dispositivo devido aos requisitos do fim de vida útil ou da concessão.

    IMPORTANTE Para uma solicitação de uma Exclusão de Dados de Fim de Concessão/Vida Útil se concluir com sucesso, o dispositivo deve estar conectado à internet através de uma conexão de rede local(LAN). Se um dispositivo estiver usando uma conexão sem fios, sua solicitação de Exclusão de Dados permanece pendente.

    – **Limpeza de Unidades por Firmware**: também conhecida como a Limpeza de BIOS Panasonic, esse tipo de Exclusão de Dados é suportado a nível do BIOS para certos dispositivos Panasonic.

    – **Dispositivo Móvel**: a operação se executa no dispositivo móvel e exclui todas as mensagens e contas de e-mail, os contatos, registros de telefone e outros tipos de dados salvos no dispositivo.
- Para filtrar por motivo, na área **e o motivo da Exclusão de Dados é** , selecione uma ou mais caixas de seleção a partir das seguintes escolhas possíveis:
  - **Desaparecido** indica que o dispositivo está perdido ou desaparecido.
  - **Final da concessão / vida**— O dispositivo está em fase final de concessão ou de vida funcional.

    IMPORTANTE Para uma solicitação de uma Exclusão de Dados de Fim de Concessão/Vida Útil se concluir com sucesso, o dispositivo deve estar conectado à internet através de uma conexão de rede local(LAN). Se um dispositivo estiver usando uma conexão sem fios, sua solicitação de Exclusão de Dados permanece pendente.
  - **Outras** representa todos os outros motivos pela solicitação da Exclusão de Dados.

4. Clique em **Mostrar Resultados** para gerar novamente o relatório usando os critérios especificados.

   O relatório do Resumo de Exclusão de Dados mostra todos os dispositivos que já tiveram a solicitação de uma Exclusão de Dados. Para cada dispositivo listado, a página Relatórios do Resumo de Exclusão de Dados inclui as seguintes informações:

- **Identificador**: o identificador do dispositivo de destino.
- **Nome da Solicitação**: o nome da solicitação da Exclusão de Dados.
- **Marca**: a marca do dispositivo de destino.
- **Modelo**: o modelo do dispositivo de destino.

- **Número de Série**: o número de série do dispositivo de destino.
- **Solicitado em**: a data e a hora quando a Exclusão de Dados foi solicitada.
- **Status**: o status atual da solicitação de Exclusão de Dados. Os valores possíveis incluem:
- **Tipo**: a política de Exclusão de Dados e as opções que foram definidas para esta solicitação.
- **Razão**: a razão para a solicitação de Exclusão de Dados.

É possível executar as seguintes tarefas adicionais no relatório gerado, se desejado:

- Para baixar o relatório, clique . Para mais informações, consulte "Baixando Relatórios" na página 150.
- Para imprimir a página atual do relatório, clique em . Para mais informações, consulte "Imprimindo Relatórios" na página 149.
- Para salvar os filtros que você usou para gerar o relatório, clique em . Para mais informações, consulte "Salvando Filtros de Relatório" na página 149.

Página Detalhes de Exclusão de Dados

A página Detalhes de Exclusão de Dados mostra as informações de configuração de cada solicitação de Exclusão de Dados. Esta página também fornece um link para o arquivo de registro de exclusões depois da operação de Exclusão de Dados se completar. Consulte "Arquivos de Registro de Exclusão" na página 293.

Para abrir a página Detalhes de Exclusão de Dados:

1. Complete as etapas na tarefa, "Visualizando o Status de Exclusão de Dados" na página 284.
2. Na página Relatório de Resumo de Exclusão de Dados, clique no link **Visualizar** para o dispositivo desejado. A página Detalhes de Exclusão de Dados é aberta, mostrando as seguintes informações:
   - **ID de Solicitação**: o número de identificação desta solicitação de Exclusão de Dados.
   - **Identificador**: o identificador do dispositivo de destino.
   - **Marca**: a marca do dispositivo de destino.
   - **Modelo**: o modelo do dispositivo de destino.
   - **Número de Série**: o número de série do dispositivo de destino.
   - **Número do Ativo**: o número de ativo do dispositivo de destino.
   - **Última Chamada**: a data e a hora (incluindo o fuso horário) da última chamada do dispositivo de destino para o Centro de Monitoramento.
   - **Motivo pela Solicitação de Exclusão de Dados**: o motivo especificado pela iniciação da operação de Exclusão de Dados neste dispositivo, que pode incluir uma das seguintes opções:
     - **Desaparecido** significa que o dispositivo está perdido, mas não furtado.
     - **Fim da concessão / Vida** significa que o dispositivo está aproximando o fim da concessão, vai ser aposentado, ou vai ser retirado de serviço.

IMPORTANTE Para uma solicitação de uma Exclusão de Dados de Fim de Concessão/Vida Útil se concluir com sucesso, o dispositivo deve estar conectado à internet através de uma conexão de rede local(LAN). Se um dispositivo estiver usando uma conexão sem fios, sua solicitação de Exclusão de Dados permanece pendente.

  - **Outro** significa que o dispositivo está sendo preparado para reatribuição ou removido por outro motivo além desses fornecidos.

- **Exclusão Perpétua**: exibe um valor de **Sim** ou **Não**, dependendo de se uma exclusão perpétua foi aplicada ou não.
- **Ignorar verificação do número de série do disco rígido**: especifica se a Exclusão de Dados deve desprezar a verificação do Número de Série do Disco Rígido (HDSN - Hard Disk Serial Number) e continuar mesmo quando o número de série do Disco Rígido for desconhecido ou se alterar durante o ciclo de vida da solicitação.

  IMPORTANTE Use a opção **Ignorar Verificação do Número de Série da Unidade de Disco Rígido** com cautela. Desprezando a verificação do HDSN antes de executar uma operação de Exclusão de Dados pode excluir dados criados ou detidos por qualquer detentor pós-perda do dispositivo ou outros discos rígidos não relacionados.

- **Número de Sobrescrição de Dados:** exibe o número de limpezas de dados selecionado. Os valores possíveis são **1**, **3**, ou **7**.
- **Tipo de Exclusão de Dados**: exibe as opções de exclusão configuradas para a solicitação, com os seguintes possíveis valores:
  - **Política Personalizada**: a operação exclui arquivos e pastas específicos.
  - **Todos os Arquivos**: a operação exclui todos os arquivos, exceto o Sistema Operacional.
  - **Todos os Arquivos - Segurança**: a operação exclui todos os arquivos, incluindo o Sistema Operacional e, depois da conclusão da primeira operação de Exclusão de Dados, limpa os discos rígidos conectados. A solicitação de Exclusão de Dados é acionada por uma violação de segurança e a necessidade de remover dados confidenciais de um dispositivo.
  - **Todos os Arquivos, Limpeza de Setores e SO**: a operação exclui todos os arquivos incluindo o Sistema Operacional e limpa o disco rígido após a conclusão da solicitação. A solicitação de Exclusão de Dados é acionada pela necessidade de aposentar o dispositivo devido aos requisitos do fim de vida útil ou da concessão.

    IMPORTANTE Para uma solicitação de uma Exclusão de Dados de Fim de Concessão/Vida Útil se concluir com sucesso, o dispositivo deve estar conectado à internet através de uma conexão de rede local(LAN). Se um dispositivo estiver usando uma conexão sem fios, sua solicitação de Exclusão de Dados permanece pendente.

  - **Limpeza de Unidades por Firmware**: também conhecida como a Limpeza de BIOS Panasonic, esse tipo de Exclusão de Dados é suportado a nível do BIOS para certos dispositivos Panasonic.
  - **Dispositivo Móvel**: a operação se executa no dispositivo móvel e exclui todas as mensagens e contas de e-mail, os contatos, registros de telefone e outros tipos de dados salvos no dispositivo.
- **Definido para a exclusão**: mostra o diretório da informação que você quer excluir.

- **Incluir Atributos de Data de Arquivo no registro de Exclusão de Dados**: indica se os atributos de data do arquivo serão incluídos no arquivo de registro de exclusões. Para mais informações, consulte "Arquivos de Registro de Exclusão" na página 293.
- **Contrato**: indica se a caixa de seleção de **Eu aceito o acordo** foi selecionada quando a solicitação foi preparada.
- **Nome do Solicitante**: mostra o nome do Administrador de Segurança ou o Usuário de Segurança Avançado que enviou a solicitação.
- **Comentário de Exclusão de Dados**: mostra o comentário feito pelo Administrador de Segurança ou o Usuário de Segurança Avançado que enviou a solicitação.
- Tabela do **Status da Exclusão de Dados**: exibe informações sobre o status da solicitação de exclusão e inclui a data e a hora de quando cada status foi alcançado. Esta tabela inclui:
    - as etapas progressivas que formam as operações de Exclusão de Dados realizadas neste dispositivo
    - o **Status** de cada operação de Exclusão de Dados
    - a **Data** no formato dd/mm/aaaa hh:mm:ss AM ou PM
    - o **Usuário** que solicitou esta operação
    - quaisquer **detalhes**

Visualizar ou Imprimir um Certificado de Exclusão de Dados de Fim de Vida Útil

Para dispositivos que estão no fim de seus ciclos de vida ou estão aproximando o fim do período de concessão, você pode solicitar uma Exclusão de Dados para remover as informações confidenciais de tais dispositivos. Em tais casos, se o tipo de Exclusão de Dados for Todos os Arquivos, Limpeza de Setores & SO, Administradores de Segurança e Usuários de Segurança Avançados podem visualizar e imprimir um Certificado de Exclusão de Dados do Fim de Vida Útil para fins de conformidade. Tais certificados são úteis para provar que o dispositivo que foi aposentado ou retirado de circulação não contém informações confidenciais.

As seguintes informações estão disponíveis no certificado:

- Informações acerca da Solicitação de Exclusão de Dados e do dispositivo, incluindo:
    - **Nome da Solicitação**: O nome da solicitação da Exclusão de Dados
    - **Identificador**: O Identificador do dispositivo
    - **Fabricante**: o nome do fabricante do dispositivo
    - **Modelo**: o nome e número do modelo do dispositivo
    - **Número de Série**: o número de série de identificação do dispositivo
    - **Etiqueta de Ativo**: qualquer etiqueta específica adicionada ao dispositivo
    - **Nome do Dispositivo**: o nome do dispositivo
    - **Tipo de Exclusão de Dados**: o tipo de solicitação de Exclusão de Dados, isto é, Todos os Arquivos, Limpeza de Setores & SO
    - **Iniciada**: a data e hora quando a solicitação de Exclusão de Dados começou a executar-se no dispositivo
    - **Terminada**: a data e hora quando a solicitação de Exclusão de Dados terminou
    - **Exclusão de Dados Lançada por**: o endereço de e-mail ou o nome de usuário do Administrador de Segurança ou o Usuário de Segurança Avançado que solicitou a operação de Exclusão de Dados

- Informações sobre o disco rígido onde a operação de Exclusão de Dados decorreu, incluindo:
  - **Unidade de disco**: o número da unidade de disco no dispositivo
  - **Modelo**: o número do modelo da unidade de disco
  - **Número de Série**: o número de série da unidade de disco
  - **Tipo de Interface**: o tipo de unidade de disco, por exemplo, se se trata de uma unidade de disco ou uma unidade de estado sólido
  - **Tamanho de Setor**: o tamanho de setores individuais na unidade de disco
  - **Setores Totais**: o número total de setores individuais na unidade de disco
  - **Setores Realocados**: o número de setores que foram realocados devido à operação de Exclusão de Dados
  - **Status de SMART Drive**: informações sobre se a unidade de disco contém Tecnologia de Auto-Monitoramento, Análise e Relatório (S.M.A.R.T - Self-Monitoring, Analysis and Reporting Technology)
  - **Tamanho**: o tamanho total da unidade de disco
  - **Velocidade da Exclusão de Dados (MB/sec)**: a velocidade em MegaBytes (MB) por segundo a que a operação de Exclusão de Dados se executou
  - **Duração de Exclusão de Dados (mm:ss)**: a duração total em minutos que levou para a operação de Exclusão de Dados se executar
  - **Status**: o status da unidade de disco, se a informação foi limpa ou não
- Informações sobre a autoridade certificadora, incluindo:
  - Nome e assinatura do Operador de Segurança de Dados, comumente também o Administrador de Segurança
  - Nome e assinatura do supervisor do Operador de Segurança de Dados

Para ver ou imprimir um Certificado do Fim de Vida Útil:

1. Na página Relatórios de Resumos de Exclusão de Dados, clique no link **Visualizar** da operação de Exclusão de Dados para qual você deseja visualizar ou imprimir o certificado de Exclusão de Dados de fim de vida útil.
2. Na página Detalhes de Exclusão de Dados, clique em **Visualizar Certificado (PDF)** para abrir o arquivo do certificado.

   NOTA Se a segurança de seu navegador estiver definida para o avisar antes de abrir ou baixar arquivos, clique em **Abrir** ou **Salvar como** para abrir ou salvar o arquivo PDF.

3. Imprima o PDF do certificado usando a impressora desejada e configurada no seu dispositivo.

Remover Detalhes de uma Operação Exclusão de Dados

Em algumas circunstâncias, você pode não precisar mais salvar os detalhes de uma Solicitação de Exclusão de Dados específica na Central do Cliente. Alguns exemplos são quando uma Solicitação de Exclusão de Dados foi cancelada, concluída ou o dispositivo foi recuperado com sucesso. É possível remover os detalhes de uma operação de Exclusão de Dados na Central do Cliente.

IMPORTANTE Tenha cuidado ao remover os detalhes de uma operação de Exclusão de Dados, pois após a sua remoção, os detalhes não podem ser recuperados.

Para remover detalhes de uma operação de Exclusão de Dados:

1. Na página Relatórios de Resumos de Exclusão de Dados, clique no link **Visualizar** da operação de Exclusão de Dados para qual você deseja remover os detalhes.

   NOTA Se você ainda não o fez, é altamente recomendado que você primeiro baixe o arquivo de registro antes de remover estes detalhes de Exclusão de Dados.

2. Na página Detalhes de Exclusão de Dados, clique em **Remover Detalhes**.
3. Uma mensagem de confirmação é aberta. Clique em **OK** para remover os detalhes da operação de Exclusão de Dados e o arquivo de registro.

Forçando a Conclusão de uma Operação de Exclusão de Dados

Não é possível ativar uma segunda operação de Exclusão de Dados em um dispositivo específico se um processo existente já estiver ocorrendo.

Se a operação de Exclusão de Dados falhar em concluir-se, você pode forçá-la a terminar, o que altera o status da operação de Exclusão de Dados no banco de dados para **Concluída**, permitindo-lhe iniciar uma nova operação de Exclusão de Dados. Fazendo isto não afeta nenhum processo que esteja atualmente em andamento em quaisquer dispositivos e não cancela nenhuma operação de Exclusão de Dados que esteja atualmente em andamento.

Depois de forçar uma operação de Exclusão de Dados a concluir-se, você não pode desfazer a alteração do status.

Para forçar a conclusão de uma operação de Exclusão de Dados:

1. Na página Relatórios de Resumos de Exclusão de Dados, clique no link **Visualizar** da operação de Exclusão de Dados cuja conclusão você deseja forçar.
2. Na página Detalhes de Exclusão de Dados, clique em **Concluir Solicitação**.
3. Na mensagem de confirmação, clique em **OK** para concluir a operação de Exclusão de Dados.

Limpar Exclusão de Dados Perpétua

Se uma solicitação de Exclusão de Dados foi enviada com a opção **Exclusão Perpétua**, é possível parar a Exclusão de Dados Perpétua no dispositivo de destino.

IMPORTANTE Exclusão de Dados Perpétua pode ser interrompida apenas após a conclusão do ciclo inicial de eliminação.

Para limpar Exclusão de Dados Perpétua:

1. Na página Relatórios de Resumos de Exclusão de Dados, clique no link **Visualizar** da operação de Exclusão de Dados que foi solicitada com a opção de Exclusão de Dados Perpétua.
2. Clique em **Limpar sinalizador de Exclusão de Dados perpétua**.
3. Na mensagem de confirmação, clique em **OK** para limpar a Exclusão Perpétua para a solicitação de Exclusão de Dados.

Excluindo ou Cancelando uma Solicitação de Exclusão de Dados

Antes da ativação da Exclusão de Dados no dispositivo de destino, a solicitação de Exclusão de Dados pode ser excluída ou cancelada, dependendo de seu status. Se o status da solicitação da Exclusão de Dados for **Rascunho**, a mesma pode ser excluída. Se o status da Exclusão de Dados for **Solicitada** ou **Definida, Aguardando Chamada**, a solicitação não pode ser excluída, mas pode ser cancelada.

As seguintes tarefas estão incluídas nesta seção:

- Excluindo um Rascunho de uma Solicitação de Exclusão de Dados
- Cancelando uma Solicitação de Exclusão de Dados para Um Único Dispositivo
- Cancelando Solicitações de Exclusão de Dados para Vários Dispositivos

Excluindo um Rascunho de uma Solicitação de Exclusão de Dados

Excluindo um rascunho de uma solicitação de Exclusão de Dados:

1. Na página Relatórios de Resumos de Exclusão de Dados, clique no link**Visualizar** do rascunho da operação de Exclusão de Dados.
2. Revise os detalhes do rascunho para garantir que esse é o que você deseja excluir.
3. Role até o final da página e clique no botão **Excluir**.
4. Na mensagem de confirmação, clique em **OK** para confirmar a operação de exclusão.

Cancelando uma Solicitação de Exclusão de Dados para Um Único Dispositivo

Para cancelar uma solicitação de Exclusão de Dados com um status de Solicitada ou Definida, aguardando chamada:

1. Na página Resumos de Exclusão de Dados, clique no link **Visualizar** da operação de Exclusão de Dados desejada.
2. Revise os detalhes da solicitação para garantir que essa é a que você deseja cancelar.
3. Clique em **Cancelar Solicitação** para cancelar a solicitação de Exclusão de Dados.
4. Na mensagem de confirmação, clique em **OK** para confirmar o cancelamento.

Cancelando Solicitações de Exclusão de Dados para Vários Dispositivos

Para cancelar várias solicitações de Exclusão de Dados com um status de Solicitada ou Definida, aguardando chamada:

1. Na página do Resumo da Exclusão de Dados, faça uma das seguintes opções:
   - Para cancelar uma ou mais operações de Exclusão de Dados, marque a caixa de seleção adjacente a cada operação de Exclusão de Dados que você deseja cancelar.
   - Para cancelar todas as operações de Exclusão de Dados na página atual, marque a caixa de seleção ao lado de **Identificador** na fila de cima da grelha de resultados.

2. Clique em **Editar Solicitações para Dispositivos Selecionados**. O diálogo Editar dispositivos selecionados se abre.
3. Na coluna **Ação** das linhas **Solicitado** e **Definido, Aguardando Chamada**, abra a lista e selecione **Cancelar Solicitação**.
4. Clique em **Enviar**. As solicitações de Exclusão de Dados para dispositivos selecionados são cancelados.

Arquivos de Registro de Exclusão

Quando uma solicitação de Exclusão de Dados é concluída, um arquivo de Registro da Exclusão é carregado para a Central do Cliente e disponibilizado na página Detalhes de Exclusão de Dados. Um arquivo de registro de exclusões fornece detalhes sobre o que foi excluído no dispositivo de destino.

NOTA Datas e horas em um arquivo de registro são exibidas no formato de Tempo Universal Coordenado (UTC).

Os arquivos de Registro de Exclusão incluem as seguintes informações sobre a operação de Exclusão de Dados:

- **Data de Conclusão**: a data e a hora de conclusão da solicitação de exclusão no dispositivo de destino.
- **Tipo de Exclusão de Dados**: indica o tipo de exclusão. Os valores possíveis são:
  - **Todos os Arquivos Exceto SO**
  - **Todos os Arquivos Incluindo SO**
  - **Arquivos/Diretórios Específicos** (apenas para computadores com Windows)
- **Motivo da Exclusão de Dados:** indica o porquê da execução da solicitação de Exclusão de Dados. Os valores possíveis são:
  - **Desaparecido**
  - **Fim de Vida Útil / Contrato de Concessão**
  - **Outro**
- **Identificador**: o identificador do dispositivo de destino.
- **Modelo**: o modelo do dispositivo de destino.
- **Marca**: a marca do dispositivo de destino.
- **Número de Série**: o número de série do dispositivo de destino.
- **Etiqueta do Ativo**: a etiqueta do ativo do dispositivo de destino, que é um número de rastreamento opcional definido pelo usuário.
- **Nome do Dispositivo**: o nome de rede do dispositivo de destino.
- **Iniciada em**: a data e a hora quando a execução da Exclusão de Dados foi iniciada no dispositivo de destino.
- **Lista de Arquivos Excluídos**: o caminho completo de todos os arquivos excluídos.
- **Finalizada**: a data e a hora do término do processo da Exclusão de Dados.
- **Sobrescrições de Dados:** o número de limpezas de dados executadas.
- **Lista de Arquivos**: uma lista de todos os arquivos excluídos durante a operação.

Se a opção **Incluir Atributos de data do Arquivo** foi selecionada quando a Exclusão de Dados foi solicitada, os atributos de data do arquivo (**Criado**, **Modificado,** and **Acessado**) para cada arquivo são listados em formato delimitado por tabulação.

NOTA Para dispositivos do Windows, a data de **Acessado** aparece apenas se a seguinte configuração estiver ativa nas Configurações de Conta: **Ativar carimbos de data/hora de último acesso de arquivo (apenas dispositivos do Windows)**. Para mais informações, consulte "Editando Configurações de Conta" na página 116.

IMPORTANTE Em um cenário pós-furto, a data de **Acesso** de um arquivo pode ser posterior à data do furto. A data de acesso não indica necessariamente se o arquivo foi comprometido após o furto. Malware não detectado, análises de antivírus e de spyware, backup automatizado e outros aplicativos similares também podem acionar uma alteração de data de **Acesso**, indicando quando o arquivo foi acessado pela última vez. Como resultado, este valor deve ser considerado útil para determinar se um arquivo não foi acessado de certeza, mas não o inverso.

- **contas de e-mail**: somente para telefones Android: uma lista de todas as contas de e-mail excluídas do dispositivo móvel durante a operação de Exclusão de Dados.
- **Data de Início de Exclusão de Arquivos Recuperáveis** se aplica apenas às opções de **Todos os Arquivos** e **Todos os Arquivos Segurança**: a data e a hora quando a operação de Exclusão de Dados começou a limpar os arquivos recuperáveis.
- **Data de Conclusão de Exclusão de Arquivos Recuperáveis** se aplica apenas às opções de **Todos os Arquivos** e **Todos os Arquivos Segurança**: indica a data e a hora quando a operação de Exclusão de Dados terminou a limpeza dos arquivos recuperáveis.

Visualizando o Arquivo de Registro de Exclusão

Quando a solicitação de Exclusão de Dados for completada, o status se atualiza para **Concluída, Arquivo de Registro Carregado** e o arquivo de exclusão se torna disponível, permitindo que você baixe e visualize os resultados da operação da Exclusão de Dados.

As seguintes tarefas estão incluídas nesta seção:

- Visualizando o Arquivo de Registro de Exclusão para Um Único Dispositivo
- Visualizando os Registros de Exclusões para Vários Dispositivos
- Visualizando o Arquivo de Registro de Exclusões em um Dispositivo Móvel

Visualizando o Arquivo de Registro de Exclusão para Um Único Dispositivo

Para baixar e visualizar o arquivo de registro de Exclusão:

1. Na página Relatório do Resumo da Exclusão de Dados, clique no link **visualizar** da operação de Exclusão de Dados desejada.
2. Na página Detalhes de Exclusão de Dados, clique em **Ver registro de exclusões**.
3. O diálogo de Baixar de Arquivo é aberta, onde você toma uma das seguintes ações:
   - Clique em **Abrir**para abrir o arquivo de registro.
   - Clique em **Salvar** para salvar o arquivo no seu dispositivo local.

O arquivo de registro está em formato de texto (.txt) e pode ser visualizado usando qualquer editor de arquivos de texto.

Visualizando os Registros de Exclusões para Vários Dispositivos

Para baixar um arquivo .ZIP contendo os arquivos de registro para várias operações de Exclusão de Dados:

1. Na página do Resumo da Exclusão de Dados, faça uma das seguintes opções:
   - Para ver o arquivo de registro para uma ou mais operações de Exclusão de Dados, marque a caixa de seleção adjacente a cada operação de Exclusão de Dados.
   - Para ver o arquivo de registro para todas as operações de Exclusão de Dados completadas na página atual, marque a caixa de seleção ao lado de **Identificador** na fila de cima da grelha de resultados.
2. Clique **Baixar Arquivos de Registro para Dispositivos Selecionados**.
3. Se o diálogo Baixar Arquivo(s) de Registro para Dispositivos Selecionados abrir, clique **Baixar**.

   NOTA Este diálogo é exibido somente se você selecionou uma ou mais operações de Exclusão de Dados que não possuam um status de **Concluída, Arquivo de Registro Carregado**.

4. O diálogo de Baixar de Arquivo é aberta, onde você toma uma das seguintes ações:
   - Clique em **Abrir** para extrair o arquivo .ZIP e ver os arquivos de registro.
   - Clique em **Salvar** para salvar o arquivo .ZIP no seu dispositivo local.

   Os arquivos de registro estão em formato de texto (.txt) e podem ser visualizados usando qualquer editor de arquivo de texto.

Visualizando o Arquivo de Registro de Exclusões em um Dispositivo Móvel

Para baixar e visualizar o arquivo de registro em um dispositivo móvel:

1. Na página Relatório do Resumo da Exclusão de Dados, clique no link **visualizar** da operação de Exclusão de Dados desejada.
2. Na página Detalhes de Exclusão de Dados, clique em **Ver registro de exclusões**.
3. No diálogo **Download de Arquivos**, clique em **Salvar** para salvar o arquivo em seu dispositivo local.
4. Salve o arquivo de registro com uma extensão de arquivo .xml

   É possível ver o arquivo de registro usando qualquer visualizador de XML ou um navegador da Web.

Capítulo 11: Gerenciando Cercas Geográficas

Os administradores podem usar o recurso de cercas geográficas para especificar limites com base em dados de rastreamento por geolocalização para rastrear dispositivos monitorados. Os recursos de Rastreamento por Geolocalização e de Cercas Geográficas da Absolute Software permitem que a sua empresa determine a localização física de um dispositivo de computação específico, com mais precisão e de imediato, de acordo com a última chamada do agente para o Centro de Monitoramento. Também é assumido que o dispositivo está corretamente equipado com um dispositivo de posicionamento aprovado para usar essas funções.

Um administrador pode especificar limites usando o editor de cercas geográficas e rastrear o movimento de dispositivos por estas localizações. Sempre que um dispositivo cruzar o limite definido usando as cercas geográficas, alertas são disparados na Central do Cliente e, dependendo das configurações especificadas na conta, resultam em notificações por e-mail enviadas a administradores e/ou outros eventos na Central do Cliente. As Cercas Geográficas estão disponíveis para todas as contas autorizadas para a função de Rastreamento por Geolocalização. Além disso, as cercas geográficas são suportadas em todos os agentes (dispositivos) na conta em que dados de rastreamento por geolocalização estão disponíveis.

Para informações sobre os requisitos de sistema para geolocalização, consulte "Compreendendo Tecnologias de Localização" na página 219.

Este capítulo inclui as seguintes seções:

Segurança de Cercas Geográficas

Devido à natureza sigilosa do Rastreamento por Geolocalização e recursos de cercas geográficas, diversas verificações de segurança foram implementadas para garantir que o serviço seja iniciado somente por indivíduos autorizados e que sua execução ocorra somente nos dispositivos de destino corretos:

- A Absolute Software deve ter um acordo de pré-autorização assinado por sua empresa nos seus registros.
- O dispositivo deve ter um agente ativado com um identificador único e dados de Rastreamento por Geolocalização válidos para ser atribuído a uma área de cerca geográfica.

Autorizando Rastreamento por Geolocalização

A Absolute Software deve ter um acordo de autorização assinado por sua empresa nos seus arquivos antes de você poder usar os recursos de Rastreamento por Geolocalização e as Cercas Geográficas Virtuais.

O Acordo de Autorização de Administração de Segurança e da Geolocalização Absolute fornece vários métodos para coletar informações específicas da sua empresa.

- Complete o Formulário de Autorização de Administração de Segurança e da Geolocalização para especificar os Administradores de Segurança para a sua conta, os quais serão autorizados a usar as operações avançadas incluídas no seu produto da Central do Cliente e para rastrear e monitorar dispositivos.
- Complete a seção do Rastreamento por Geolocalização para indicar se sua empresa vai usar a Geolocalização ou não e, se sim, se pretende habilitar todos os dispositivos ou apenas dispositivos específicos para usufruírem deste recurso.
- Complete a seção da Autorização e das Assinaturas para especificar os Responsáveis Assinantes da sua empresa que aceitam a utilização por sua empresa das operações de segurança avançadas, de acordo com os termos deste acordo.

Para baixar uma cópia em branco do acordo de autorização, siga as instruções na tarefa, "Baixando e Enviando o Acordo de Autorização" na página 259.

Usando a Tecnologia de Cercas Geográficas

As Cercas Geográficas são primariamente usadas como blocos de construção das políticas de segurança baseadas na localização de dispositivos. As Cercas Geográficas, em combinação com o Rastreamento por Geolocalização, podem ser usadas para marcar a localização de um dispositivo e, consequentemente, garantir que a segurança desses dispositivos não seja violada. Por exemplo, uma cerca geográfica especificando todo o estado de Nova Iorque como uma zona segura e um alerta que a acompanha na Central do Cliente são criados para a Conta A. Quando um dos dispositivos na Conta A viaja para fora do estado de Nova Iorque, todos os administradores dessa conta são alertados através de uma notificação por e-mail automatizada. Dependendo do local e do status de segurança do dispositivo, o administrador pode escolher implementar outras medidas de segurança, tais como a execução da Exclusão de Dados ou a solicitação de um congelamento do dispositivo.

Para usar cercas geográficas de forma efetiva, você cria primeiro uma cerca geográfica, e, depois, cria um alerta que se liga à cerca geográfica. Quando você cria um alerta associado a uma cerca geográfica, é necessário especificar as regras para acionar o alerta com base nas seguintes opções:

- **Localização**:
  - **Fora**: Cria um alerta sempre que um dispositivo se desloca para fora dos limites da cerca geográfica.
  - **Dentro**: Cria um alerta sempre que um dispositivo se desloca para dentro dos limites da cerca geográfica.
- **Nome da Cerca Geográfica Virtual**: A cerca geográfica ao qual pertence o alerta.
- **Duração**: O período de tempo necessário para acionar o alerta, após as regras especificadas serem quebradas. É possível especificar a duração do tempo em horas, dias ou semanas.

Para configurar uma Cerca Geográfica funcional:

1. Crie uma Cerca Geográfica Virtual desejada usando a página Criar e Editar Cercas Geográficas Virtuais. Para mais informações, consulte "Criando Cercas Geográficas" na página 299.

   NOTA Se uma cerca geográfica que corresponde aos seus critérios já existe, você não precisa criar uma nova.

2. Crie um alerta baseado na Cerca Geográfica recém-criada usando a página Criar e Editar Alertas. Na lista de **Campo**, selecione o valor de **Localização** e, em seguida, especifique as regras desejadas.

   Para mais informações sobre a criação de Alertas, consulte "Criando Novos Alertas Personalizados" na página 43.

Compreendendo Mapas de Geolocalização

Mapas de Geolocalização aparecem em quaisquer páginas de geolocalização dentro da Central do Cliente. Essas páginas incluem:

- A página **Criar e editar Cercas Geográficas**, que mostra o Editor de Cercas Geográficas. É possível usar o editor de cercas geográficas para adicionar, editar e localizar cercas geográficas em um mapa.
- **Relatórios de Rastreamento por Geolocalização**, que permitem a visualização de informações de localização dos seus dispositivos. As cercas geográficas criadas para a sua conta aparecem nos relatórios de rastreamento por geolocalização. Para mais informações, consulte "Relatórios de Rastreamento de Geolocalização" na página 217.

NOTA O editor de cercas geográficas e os relatórios de rastreamento por geolocalização usam o Google Maps™. Se o Google Maps é proibido no seu país (determinado pelo endereço IP do seu computador), mapas ESRI® serão utilizados em vez. Para mais informações sobre como usar os mapas ESRI, vá para www.esri.com.

Ferramentas de Navegação do Mapa

As seguintes ferramentas de navegação do Google Maps estão disponíveis:

Ferramenta	Descrição
Movimento Panorâmico	Use a ferramenta de movimentos panorâmicos para uma área específica do mapa. Clique em uma ou mais das setas até a área desejada estar em vista. Esta ferramenta é tipicamente usada em conjunto com a ferramenta de Zoom.
Zoom	Use a ferramenta de Zoom para ampliar ou reduzir áreas específicas do mapa. ● Para ampliar o zoom, clique em + repetidamente, ou desloque o controle deslizante em direção ao botão. É também possível ampliar o zoom clicando duas vezes no mapa ou usando a roda de rolagem de seu mouse. ● Para reduzir o zoom, clique em − repetidamente, ou desloque o controle deslizante em direção ao botão. É possível reduzir o zoom ao usar a roda de rolagem de seu mouse.
Mapa | Selecionador de Satélite	Usar o mapa | Ferramenta de satélite para selecionar o tipo de mapa. Para selecionar um tipo de mapa, execute uma das seguintes ações: ● Para mostrar um mapa de ruas, clique em **Mapa**. Esta é a opção padrão. ● Para mostrar um mapa com informações de relevo e vegetação, clique em **Mapa** e selecione **Relevo**. ● Para mostrar um mapa de imagens de satélite, clique em **Satélite**. ● Para mostrar um mapa de imagens de satélite com nomes de localidades, clique em **Satélite** e selecione **Etiquetas**.

Ferramentas das Cercas Geográficas

Os seguintes controles estão disponíveis para adicionar, editar e localizar cercas geográficas:

Ferramenta de cercas geográficas	Descrição
Ir para o endereço	Use a ferramenta Ir para Endereço para visualizar uma localização específica no mapa. Para encontrar um local, clique no ícone, insira o endereço do local no campo fornecido e pressione `Enter`. Para obter maior precisão, forneça uma morada física, bem como nomes de cidade e estado.
Encontrar limites e marcadores:	Se múltiplos limites aparecem num mapa, use a ferramenta Localizar Limites e Marcadores para ver os limites individualmente. Clique no ícone repetidamente para percorrer cada limite e marcador no mapa.
Traçar um Limite	Use a ferramenta Desenhar um Limite para criar novos polígonos de limites que definem a cerca geográfica. Para criar um polígono de limites clique no ícone e depois clique no mapa onde deseja iniciar o polígono. Para instruções detalhadas, consulte "Criando Cercas Geográficas" na página 299.
Editar um Limite	Use a ferramenta Editar um Limite para editar um polígono de limites existente. Para alterar o tamanho ou a forma de um polígono de limites, clique no ícone e depois clique no polígono que deseja editar. Para instruções detalhadas, consulte "Editando Cercas Geográficas" na página 301.
Remover um Limite	Use a ferramenta Remover um Limite para excluir um polígono de limites na sua conta. Para excluir um polígono de limites, clique no ícone e depois clique no polígono que deseja remover.

Criando Cercas Geográficas

É possível usar a página Criar e Editar Cercas Geográficas para definir os limites de uma nova cerca geográfica.

Uma cerca geográfica pode incluir um polígono de limite único que cobre uma área ou é possível desenhar vários polígonos e incluir várias áreas numa só cerca geográfica.

IMPORTANTE As seguintes instruções assumem que você já assinou o Acordo de Autorização de Administração de Segurança e da Geolocalização e já o entregou à Absolute Software. Para mais informações, consulte "Baixando e Enviando o Acordo de Autorização" na página 259. Além disso, a primeira vez que você acessar qualquer página de cercas geográficas durante uma sessão de login, uma página de confirmação solicitará a aceitação dos Termos e Condições de uso.

Para criar uma cerca geográfica para dispositivos na sua conta:

1. No painel de navegação, clique em **Administração** > **Cercas Geográficas** > **Criar e Editar Cercas Geográficas**.
2. Quando solicitado, aceite o uso do recurso de Rastreamento por Geolocalização.

3. Na página Criar e Editar Cercas Geográficas Virtuais, nos campos **Nome da Cerca Geográfica Virtual** e **Descrição da Cerca Geográfica Virtual**, digite um nome e descrição para a nova Cerca Geográfica.
4. Para considerar somente locais de dispositivos coletados que tenham uma alta probabilidade de serem precisos em relação à cerca geográfica, selecione **Testar apenas locais com elevados níveis de confiança em relação aos limites das cercas geográficas** na área **Níveis de Confiança Aplicáveis** .
5. Na área **Tecnologias de Localização Aplicáveis**, selecione as tecnologias de localização que deseja aplicar à cerca geográfica. Para mais informações sobre tecnologias de localização que podem ser usadas pela Central do Cliente, consulte "Compreendendo Tecnologias de Localização" na página 219.

   Se a opção de Posicionamento Wi-Fi do Google Maps™ estiver acinzentada, esta tecnologia de localização não está ativada na sua conta. Para ativar esta tecnologia para todas as cercas geográficas novas e existentes, consulte "Gerenciando Configurações de Conta" na página 116.

   IMPORTANTE A georesolução IP tem na melhor das hipóteses precisão até ao nível de cidade, e varia do nível de cidade ao nível de país. Portanto, não ative a georesolução IP para cercas geográficas pequenas.

6. Crie um polígono de limites usando o mapa e as ferramentas no Editor de Cercas Geográficas, da seguinte forma:
   a) Use as ferramentas de navegação do mapa para mostrar a área no mapa onde deseja criar um limite. Para mais informações sobre as ferramentas de navegação, consulte "Ferramentas de Navegação do Mapa" na página 298.
   b) Clique .
   c) Clique no local no mapa onde deseja iniciar o polígono.
   d) Clique no local no mapa onde deseja criar o primeiro canto. O primeiro lado do polígono é adicionado ao mapa.
   e) Use o método descrito na etapa d para criar cada lado do polígono, exceto o lado final.
   f) Para completar o polígono, clique duas vezes no ponto final do último lado que você criou. O polígono está fechado.

   IMPORTANTE As linhas de um polígono de limites não podem se cruzar ou interceptar, exceto nos pontos finais. Para compensar as limitações de precisão da tecnologia de localização, desenhe um polígono de limites ligeiramente maior do que é necessário.

7. Repita Etapa 6 para cada polígono de limites que você deseja incluir nesta cerca geográfica.
8. Clique em **Salvar**.

   A página Visualizar e Gerenciar Cercas Geográficas se abre com a nova cerca geográfica exibida na tabela Cercas Geográficas. Cercas Geográficas que são demasiado pequenas para aparecerem com precisão em um nível de zoom específica aparecem no mapa como marcadores pequenos e redondos.

Visualizando Cercas Geográficas

A página Visualizar e Gerenciar Cercas Geográficas Virtuais permite que você visualize um resumo de todas as Cercas Geográficas que atendem ao critério de pesquisa especificado.

Para visualizar uma Lista de Cercas Geográficas Existentes na sua conta:

1. No painel de navegação, clique **Administração** > **Cercas Geográficas Virtuais** > **Ver e Gerenciar Cercas Geográficas Virtuais**.
2. Quando solicitado, aceite o uso do recurso de Rastreamento por Geolocalização.
3. Na página Ver e Gerenciar Cercas Geográficas Virtuais, no campo **Nome da Cerca Geográfica Virtual**, digite todo ou parte do nome da cerca geográfica virtual que você deseja ver e clique em **Mostrar resultados**.

   A página Visualizar e Gerenciar Cercas Geográficas Virtuais se atualiza e mostra uma lista de todas as Cercas Geográficas que atendem ao critério de pesquisa especificado na grelha de resultados
4. Clique no link de **Nome**, que abre a página Criar e Editar Cercas Geográficas Virtuais para a Cercas Geográficas.

Editando Cercas Geográficas

É possível editar as propriedades e configurações de uma cerca geográfica. É também possível usar o editor de cercas geográficas para mover, alterar a forma e excluir polígonos de limites de uma cerca geográfica existente.

Para editar uma cerca geográfica existente:

1. Abra a cerca geográfica que você deseja editar. Para mais informações, consulte "Visualizando Cercas Geográficas" na página 301.
2. Na página Criar e Editar Cercas Geográficas, edite os valores nos campos **Nome da Cerca Geográfica** e **Descrição da Cerca Geográfica**, se necessário.
3. Atualize as seleções na área **Níveis de Confiança Aplicáveis** e na área **Tecnologias de Localização Aplicáveis**, se necessário.
4. Para alterar o tamanho ou a forma de um polígono de limites:

   a) Clique .
   b) Clique no polígono que você deseja editar. Alças aparecem nos cantos do polígono e nos pontos centrais de cada linha.
   c) Clique em uma alça e arraste-a para sua nova localização. Para desfazer uma alteração, clique em .
   d) Repita Etapa c até que o polígono atinja o tamanho e forma necessários.
5. Para mover o polígono de limites:

   a) Clique .
   b) Clique no polígono que você deseja editar. Alças aparecem nos cantos do polígono e nos pontos centrais de cada linha.

c) Clique em qualquer parte do polígono e arraste-o para sua nova localização.

6. Para remover um polígono de limites:

    a) Clique .
    b) Clique no polígono que você deseja remover.

7. Clique em **Salvar**. Os dados de Cercas Geográficas são atualizados e a página Visualizar e Gerenciar Cercas Geográficas se abre e exibe os valores editados na grelha de resultados.

Excluindo Cercas Geográficas

IMPORTANTE Não é possível excluir cercas geográficas que estão associadas a um ou mais alertas.

Para excluir uma cerca geográfica:

1. Abra a cerca geográfica que você deseja excluir. Para mais informações, consulte "Visualizando Cercas Geográficas" na página 301.
2. Na página Criar e Editar Cercas Geográficas, clique em **Excluir**. A página Visualizar e Gerenciar Cercas Geográficas se abre e a cerca geográfica é excluída da grelha de resultados.

Capítulo 12: Usando o Congelamento de Dispositivo

A função de Congelamento de Dispositivo permite aos Administradores de Segurança e aos Usuários de Segurança Avançados da Central do Cliente selecionar dispositivos específicos e mostrar uma mensagem de tela cheia, restringindo usuários de operar o dispositivo. O Congelamento de Dispositivo acontece a nível de sistema operacional (OS) e, quando ele está ativo, a Central do Cliente mostra uma mensagem em tela cheia no dispositivo. Quando você congela um dispositivo, apenas a mensagem selecionada é mostrada na tela e nenhum componente do Windows (como o Gerenciador de Tarefas) estará acessível. O Windows continua rodando em segundo plano e o usuário pode alternar entre as janelas, pressionando as teclas **ALT+TAB** para salvar qualquer documento aberto ou fechar qualquer janela aberta no momento.

O recurso Congelamento de Dispositivo é persistente. O estado de congelamento persiste em reinicializações de dispositivos mesmo quando o dispositivo for reiniciado em modo de segurança. O congelamento reaparece quando o SO é carregado novamente. Se um usuário reinstalar o SO, o dispositivo congela novamente quando o agente se auto-reparar.

Os administradores de segurança e os usuários de segurança avançados podem usar a Central do Cliente para gerenciar o Congelamento de Dispositivo das seguintes formas:

- Enviar solicitações de Congelamento de Dispositivo
- Criar e gerenciar políticas de Congelamento de Dispositivo do estado offline
- Rastrear o status de Congelamento de Dispositivo de dispositivos
- Descongelar um dispositivo congelado

Para mais informações sobre as operações de segurança que estas funções de usuário podem executar, consulte "Funções de usuário e seus direitos de acesso" na página 96.

Este capítulo inclui as seguintes seções:

- Requisitos Mínimos do Sistema
- Trabalhando com Solicitações de Congelamento de Dispositivo
- Gerenciando Políticas do Congelamento de Dispositivo do Estado Offline
- Rastreamento do Status de Congelamento de Dispositivos
- Descongelando um Dispositivo Congelado
- Gerenciando Mensagens Personalizadas de Congelamento de Dispositivo

NOTA Usuários de segurança avançados podem executar operações de congelamento de dispositivos apenas em aqueles dispositivos que pertencem ao grupo de dispositivos a que estes usuários foram atribuídos.

Requisitos Mínimos do Sistema

Atualmente, a função Congelamento de Dispositivo está disponível para dispositivos que atendem aos seguintes requisitos mínimos do sistema:

- **Sistemas Operacionais**: o dispositivo de destino deve estar executando uma versão suportada de um dos seguintes sistemas operacionais:
  - Windows
  - Mac OS X

NOTA Políticas de Congelamento de Dispositivos do estado offline são apenas suportadas em dispositivos do Windows.

Para mais informações, consulte "Plataformas Suportadas para o Agente Computrace" na página 22.

- **Agente Computrace**: o dispositivo de destino deve ter um status de agente de Ativo, o que significa que o agente Computrace está instalado e está chamando regularmente para o Centro de Monitoramento da Absolute. Para informações sobre as versões mais recentes do agente, consulte "Baixando o Agente Computrace" na página 127.

Trabalhando com Solicitações de Congelamento de Dispositivo

Pessoal de segurança autorizado pode lançar uma solicitação de congelamento de dispositivo, que está associada a uma mensagem de congelamento de dispositivo, em qualquer dispositivo em sua conta. Você precisa de um código de autorização para solicitar um Congelamento de Dispositivo. Para mais informações, consulte "Solicitando um Código de Autorização de Segurança" na página 265.

Depois de iniciada, a operação de congelamento de dispositivos será executada na próxima chamada do agente, mesmo se o usuário não fizer login no sistema operacional. Se uma reinicialização do sistema interromper a operação de Congelamento do Dispositivo, o congelamento persiste no dispositivo ao reiniciar e quando o sistema operacional for carregado. Quando um dispositivo é congelado, você pode usar a Central do Cliente para descongelá-lo ou gerar um código de acesso para permitir que usuários descongelem o dispositivo manualmente. Para mais informações, consulte os seguintes tópicos:

- "Visualizando o Código de Acesso do Descongelamento" na página 329
- "Descongelando um Dispositivo Congelado" na página 327

IMPORTANTE Se você iniciar um congelamento de dispositivo em um dispositivo com uma solicitação de Exclusão de Dados pendente ou iniciar uma solicitação de Exclusão de Dados em um dispositivo com uma solicitação de congelamento de dispositivo pendente, a solicitação de congelamento de dispositivo se executa depois da conclusão da solicitação da Exclusão de Dados.

Além disso, você não pode iniciar um congelamento de dispositivo em um dispositivo com um relatório de furto aberto. Se você escolher implementar o Congelamento de Dispositivo em um dispositivo furtado sem um Relatório de Furto, você deve descongelar o dispositivo antes de preencher o Relatório de Furto. Consulte seu *Contrato de Serviço do Usuário Final* para mais informações.

Esta seção oferece informações acerca dos seguintes tópicos:

- Solicitar um Congelamento de Dispositivo
- Cancelando uma Solicitação de Congelamento de Dispositivo
- Removendo Detalhes de uma Solicitação de Congelamento de Dispositivo

Solicitar um Congelamento de Dispositivo

NOTA As seguintes instruções assumem que você já assinou e entregou o Acordo de Autorização de Administração de Segurança e da Geolocalização da Absolute à Absolute Software e que já selecionou o seu método de autenticação de segurança. Para mais informações, consulte "Acordo de Autorização de Administração de Segurança e da Geolocalização" na página 259.

Para solicitar um Congelamento de Dispositivo:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Solicitar Congelamento de Dispositivo**. A página Solicitar Congelamento de Dispositivo se abre.
3. Se seu método de autenticação de segurança é o envio de códigos de autenticação de segurança por e-mail, na área **Solicitar Código de Autorização**, clique em **Solicitar Código**.

   A Central do Cliente mostra uma mensagem confirmando que um código de autorização foi solicitado e enviado ao endereço de e-mail. Procure a mensagem no seu e-mail.
4. No campo **Nome da Solicitação**, digite um nome apropriado para sua solicitação de Exclusão de Dados. Este valor não precisa ser único.
5. Clique em **Selecionar Dispositivos**.
6. No diálogo de Selecionar dispositivos, faça o seguinte:
   a) No campo **Onde o grupo é**, abra a lista e selecione o Grupo de Dispositivos que deseja congelar.

      NOTA Se você estiver conectado como um usuário de segurança avançado, pode selecionar apenas o Grupo de Dispositivos a que está atribuído.

   b) No campo **e qualquer campo inclui**, você pode digitar detalhes específicos para mostrar apenas aqueles dispositivos que atendem aos critérios específicos.

      Por exemplo, se você quiser mostrar apenas os dispositivos onde o campo de **Nome de Usuário** começa com a palavra “Absolute”, no campo **e qualquer campo inclui** insira **Absolute**.
   c) Clique em **Filtrar**. A caixa de diálogo Selecionar Dispositivos atualiza-se e mostra uma lista de dispositivos que satisfazem os seus critérios.
   d) Selecione os dispositivos apropriados fazendo uma das seguintes ações:
      - Para selecionar dispositivos individuais, marque as caixas de seleção para cada dispositivo.
      - Para selecionar todos os dispositivos exibidos nesta página, marque a caixa de seleção no cabeçalho.
      - Para selecionar todos os dispositivos neste grupo de dispositivos, passa com o mouse por cima da seta para baixo na caixa de seleção no cabeçalho. Clique em **Selecionar <n> Registros** (onde <n> é o número de registros) para selecionar todos os dispositivos que atendem aos critérios de filtro que você definiu anteriormente.
   e) Com os dispositivos desejados selecionados, clique em **Selecionar Dispositivos**. A página Solicitar Congelamento de Dispositivo se atualiza com uma lista de todos os dispositivos selecionados.

   NOTA Se você achar que a lista de dispositivos selecionados inclui dispositivos que foram incluídos por engano, você pode remover esses dispositivos da lista. Para remover estes dispositivos, clique no link **Remover** na última coluna do dispositivo em questão. A página Solicitar Congelamento de Dispositivo atualiza-se e mostra a lista atualizada de dispositivos.

7. No campo **Selecionar uma mensagem**, abra a lista e selecione a mensagem que deseja associar com esta solicitação de Congelamento de Dispositivo. A Central do Cliente mostra uma pré-visualização da mensagem no campo **Pré-visualização da mensagem**.

8. Na área **Selecione uma Opção de Código de Acesso**, selecione uma das seguintes opções:

   - **Gerar um código de acesso aleatório e diferente para cada dispositivo** para gerar automaticamente e utilizar um código de acesso diferente para cada um dos dispositivos de destino.
   - **Gerar o mesmo código de acesso aleatório para cada dispositivo** para gerar automaticamente e usar o mesmo código de acesso para cada um dos dispositivos de destino.
   - **Especifique um código de acesso com 8 dígitos para cada dispositivo** para usar um código de acesso previamente gerado ou personalizado. Clique no campo e insira (ou copie e cole) o código de acesso para cada dispositivo. Para mais informações, consulte "Visualizando o Código de Acesso do Descongelamento" na página 329.

9. Se o seu dispositivo de destino estiver executando o sistema operacional Windows, marque a caixa de seleção **Forçar Reinicialização** para forçar o dispositivo a reinicializar-se quando a solicitação de congelamento de dispositivo for implantada.

   Por padrão, dispositivos que rodam sistemas operacionais Mac reiniciam automaticamente quando a solicitação de Congelamento do Dispositivo é executado. Marcando esta caixa de seleção para dispositivos com Windows reinicializa o dispositivo e exibe a mensagem de Congelamento de Dispositivo sem necessitar que o usuário se conecte ao sistema operacional. A opção **Forçar uma Reinicialização** permite a você forçar uma reinicialização automática para que os usuários não possam alternar entre aplicativos e salvar seu trabalho.

10. Clique em **Enviar** para atualizar a página Solicitar Congelamento de Dispositivo e mostrar a área **Fornecer Autenticação**, onde você faz uma das seguintes ações:

    - Se seu método de autenticação de segurança é códigos de autorização enviados por e-mail, digite sua **senha da Central do Cliente** e seu **Código de Autorização**.
    - Se seu método de Autenticação de segurança for tokens RSA SecurID, digite sua **senha da Central do Cliente** e seu **código de token SecurID**.

    Para mais informações, consulte "Métodos de Autenticação de Segurança" na página 263.

11. Clique em **OK**.

    A solicitação de Congelamento de Dispositivo é criada e implementada em cada dispositivo na próxima chamada do agente.

    IMPORTANTE Depois de clicar em **OK** na página Fornecer Autenticação, a Solicitação de Congelamento de Dispositivo não poderá ser alterada. Entretanto, você pode cancelar a solicitação, desde que a mesma não tenha sido inicializada no dispositivo de destino. Consulte "Gerenciando Mensagens Personalizadas de Congelamento de Dispositivo" na página 331.

    Se o dispositivo está habilitado com a RTT, será aberta um diálogo solicitando que você force uma chamada para o dispositivo usando as MCIC. Se necessário, force uma chamada para o dispositivo. Para mais informações, consulte "Iniciando uma Chamada Forçada" na página 247.

    Quando o dispositivo recebe e processa a mensagem SMS , dependendo dos padrões do Congelamento de Dispositivo definidos para a conta, o dispositivo é congelado.

Cancelando uma Solicitação de Congelamento de Dispositivo

Na Central do Cliente, você não poderá apresentar um Relatório de Furto para um dispositivo furtado até todas as solicitações de congelamento pendentes serem concluídas ou canceladas.

Se o dispositivo estiver congelado, você necessita descongelá-lo antes de poder indicar que foi **Furtado** no Relatório de Furto. Para iniciar uma solicitiação de descongelamento para repor o dispositivo em um estado operacional, siga a tarefa, "Descongelando um Dispositivo Congelado" na página 327.

IMPORTANTE Você só pode cancelar uma solicitação de congelamento de dispositivos antes de a mesma ser implantada no dispositivo de destino; portanto a solicitação de congelamento de dispositivos deve possuir o status de **Congelamento Solicitado**.

Você pode cancelar o pedido de congelamento de dispositivo para um único dispositivo ou para vários dispositivos:

- Cancelando uma Solicitação de Congelamento de Dispositivo para um Único dispositivo
- Cancelando a Solicitação de Congelamento de Dispositivo para Vários Dispositivos

Cancelando uma Solicitação de Congelamento de Dispositivo para um Único dispositivo

Para cancelar uma Solicitação de Congelamento de Dispositivo para um único dispositivo:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Relatório do Resumo de Congelamento de Dispositivo**.
3. Na página Relatório do Resumo de Congelamento de Dispositivo, na área **Critérios de Pesquisa**, digite todos os critérios desejados e clique em **Mostrar Resultados**.

   O relatório do resumo do congelamento de dispositivos se atualiza e a grelha de resultados mostra uma lista de todos os dispositivos em sua conta que contêm uma solicitação de congelamento de dispositivo.
4. No lado da extrema direita da grelha, clique no link **Editar** do dispositivo apropriado.
5. A página Detalhes do Congelamento de Dispositivo é aberta e mostra os detalhes da solicitação selecionada. Clique em **Cancelar Solicitação**. A solicitação de Congelamento de Dispositivo é cancelada.

Cancelando a Solicitação de Congelamento de Dispositivo para Vários Dispositivos

Para cancelar pedidos de Congelamento de Dispositivo para vários dispositivos ao mesmo tempo:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Relatório do Resumo de Congelamento de Dispositivo**.
3. Na página Relatório do Resumo de Congelamento de Dispositivo, na área **e o Status de Congelamento do Dispositivo é**, marque a caixa de seleção de **Congelado** e desmarque outras caixas de seleção.

4. Digite todos os outros critérios desejados e clique em **Mostrar Resultados**.

   O Relatório do Resumo de Congelamento de Dispositivo se atualiza e a grelha de resultados mostra uma lista de todos os dispositivos em sua conta que correspondem a seus critérios de pesquisa.

5. Selecione os dispositivos em uma das seguintes formas:

   - **Somente Este Página**: na coluna da extrema esquerda da linha de cima da grelha de resultados, marque a caixa de seleção para selecionar apenas aqueles dispositivos que aparecem na página atual da grelha de resultados do Relatório do Resumo de Congelamento de Dispositivo.
   - **Selecionar Todos os Registros**: focalize seu mouse sobre o botão de lista na coluna da extrema esquerda da linha superior da grelha de resultados e clicando no link **Selecionar Todos os Registros <n>**, onde <n> é o número total de dispositivos que atendem a seus critérios de filtro. Estes dispositivos aparecem em páginas diferentes da grelha de resultados do Relatório do Resumo de Congelamento de Dispositivo.

   O relatório do resumo de congelamento do dispositivos se atualiza e mostra as caixas de seleção marcadas para dispositivos selecionados.

6. Clique em **Editar dispositivos selecionados** para abrir o diálogo Editar Dispositivos Selecionados.
7. Na coluna **Ação** da linha **Congelamento Solicitado**, abra a lista e selecione **Cancelar Solicitação**.
8. Clique em **Enviar**. As solicitações de Congelamento de Dispositivo para todos os dispositivos selecionados serão canceladas.

Removendo Detalhes de uma Solicitação de Congelamento de Dispositivo

Em algumas circunstâncias, você pode não precisar mais salvar os detalhes de uma Solicitação de Congelamento de Dispositivo específica na Central do Cliente. Alguns exemplos incluem quando uma Solicitação de Congelamento de Dispositivo foi cancelada ou concluída ou quando o dispositivo foi recuperado com sucesso.

AVISO! Tenha cuidado ao remover os detalhes de uma solicitação de Congelamento de Dispositivo porque, uma vez removidos, você não poderá restaurar estes detalhes.

É possível remover os detalhes da solicitação de Congelamento de Dispositivo para um único dispositivo ou para vários dispositivos:

- Removendo Detalhes de uma Solicitação de Congelamento de Dispositivo Único
- Removendo Detalhes de Solicitações de Congelamento de Múltiplos Dispositivos

Removendo Detalhes de uma Solicitação de Congelamento de Dispositivo Único

Para remover detalhes de uma solicitação de Congelamento de um único Dispositivo:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Relatório do Resumo de Congelamento de Dispositivo**.

3. Na página do Relatório do Resumo de Congelamento de Dispositivo, insira todos os critérios desejados e clique em **Mostrar Resultados**.

   O relatório do resumo do congelamento de dispositivos se atualiza e a grelha de resultados mostra uma lista de todos os dispositivos em sua conta que contêm uma solicitação de congelamento de dispositivo.

4. Clique no link **Ver** ou **Editar** para a solicitação desejada. A página Detalhes do Congelamento de Dispositivo é aberta e mostra os detalhes da solicitação selecionada.
5. Clique em**Remover Detalhes**. A página Confirmação de Remoção dos Detalhes do Congelamento de Dispositivo é aberta.
6. Clique em **OK**. Os detalhes da Solicitação de Congelamento de Dispositivo são excluídos da Central do Cliente.

Removendo Detalhes de Solicitações de Congelamento de Múltiplos Dispositivos

Para remover os detalhes de múltiplas solicitações de congelamento de dispositivos:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Relatório do Resumo de Congelamento de Dispositivo**.
3. Na página Relatório do Resumo de Congelamento de Dispositivo, na área **e o Status de Congelamento do Dispositivo é**, marque as caixas de seleção **Descongelado com Chamada de Agente**, **Solicitação Cancelada** e **Descongelado com Código de Acesso**. Desmarque todas as outras caixas de seleção.
4. Digite todos os critérios desejados nesta página e, em seguida, clique em**Mostrar Resultados**.

   O Relatório do Resumo de Congelamento de Dispositivo se atualiza e a grelha de resultados mostra uma lista de todos os dispositivos em sua conta que correspondem a cada status de congelamento de dispositivo selecionado.

5. Selecione os dispositivos em uma das seguintes formas:
   - **Somente Este Página**: na coluna da extrema esquerda da linha de cima da grelha de resultados, marque a caixa de seleção para selecionar apenas aqueles dispositivos que aparecem na página atual da grelha de resultados do Relatório do Resumo de Congelamento de Dispositivo.
   - **Selecionar Todos os Registros** ao focalizar seu mouse sobre o botão de lista na coluna da extrema esquerda da linha superior da grelha de resultados e clicando no link **Selecionar Todos os Registros <n>**, onde <n> é o número total de dispositivos que atendem a seus critérios de filtro. Estes dispositivos aparecem em páginas diferentes da grelha de resultados do Relatório do Resumo de Congelamento de Dispositivo.

   O relatório do resumo de congelamento do dispositivos se atualiza e mostra as caixas de seleção marcadas para dispositivos selecionados.

6. Clique em **Editar dispositivos selecionados** para abrir o diálogo Editar Dispositivos Selecionados.
7. Na lista de **Ação** para cada status de dispositivo, selecione **Remover Detalhes**.

8. Clique em **Enviar**. Os detalhes da Solicitação de Congelamento de Dispositivo para todos os dispositivos selecionados são excluídos da Central do Cliente.

Gerenciando Políticas do Congelamento de Dispositivo do Estado Offline

Pessoal de segurança autorizado pode criar uma política de Congelamento de dispositivos do estado offline para congelar dispositivos que não entraram em contato com o Centro de Monitoramento durante um período de tempo específico. Políticas do estado offline asseguram que seus dispositivos gerenciados estejam protegido mesmo quando os dispositivo estejam desligados ou quando uma conexão à rede não está disponível.

Dependendo das necessidades da sua empresa, você poderá desejar criar uma política do estado offline e aplicá-la a todos seus dispositivos gerenciados ou criar várias políticas do estado offline, com configurações diferentes, e atribuir grupos de dispositivos a cada uma delas. É também possível designar uma política do estado offline como a política padrão a ser aplicada automaticamente a dispositivos recém-ativados.

Uma nova política do estado offline é ativada nos seus dispositivos associados na próxima chamada do agente. O cronômetro da política começa então a fazer uma contagem regressiva em cada dispositivo. É possível definir o período do cronômetro para qualquer valor entre 4 dias e 365 dias e será redefinido após cada chamada de agente bem-sucedida. Se um dispositivo não entrar em contato com o Centro de Monitoramento antes do período do cronômetro expirar, o dispositivo será congelado e uma notificação por e-mail será enviada para o administrador de segurança ou ao usuário de segurança avançado que criou a política do estado offline.

Os dispositivos que são congelados por uma política do estado offline são incluídos no relatório do resumo do congelamento de dispositivos. É possível ver estes dispositivos e descongelá-los conforme necessário.

NOTA Políticas de Congelamento de Dispositivos do estado offline são apenas suportadas em dispositivos do Windows.

Esta seção oferece informações acerca dos seguintes tópicos:

- Criando uma Política de Congelamento de Dispositivos do Estado Offline
- Trabalhando com Políticas do Estado Offline Existentes
- Pesquisando uma Política de Congelamento de Dispositivo do Estado Offline
- Editando uma Política de Congelamento de Dispositivo do Estado Offline
- Designando uma Política Padrão do Estado Offline
- Gerenciando Dispositivos Associados a uma Política de Congelamento de Dispositivos do Estado Offline
- Excluindo uma Política de Congelamento de Dispositivo do Estado Offline

Criando uma Política de Congelamento de Dispositivos do Estado Offline

Para criar uma política de congelamento de dispositivos do estado offline e atribuir dispositivos a ela:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.

2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivos** > **Criar Política de Congelamento de Dispositivos**.
3. Se seu método de autenticação de segurança é o envio de códigos de autenticação de segurança por e-mail, na área **Solicitar Código de Autorização**, clique em **Solicitar Código**.

   A Central do Cliente mostra uma mensagem confirmando que um código de autorização foi solicitado e enviado ao endereço de e-mail. Procure a mensagem no seu e-mail.
4. Sob Informações da Política, insira as seguintes informações:
   a) Digite um nome no campo **Nome de Política** e clique no link **Verificar a disponibilidade do nome** para verificar se o nome que digitou não está em uso.
   b) Digite uma **Descrição da Política**.
   c) No campo **Período do Cronômetro**, digite o número de dias que devem passar antes de um dispositivo associado a esta política ser congelado. Valores entre **4** dias e **365** dias são suportados.
5. Clique no campo **Mensagem de Congelamento** e selecione a mensagem que deseja exibir no dispositivo quando ele é congelado. O texto da mensagem aparece no campo **Visualização da mensagem**.

   Se a mensagem apropriada não existir, clique no link **Criar mensagem** para criar uma nova mensagem. Para mais informações, consulte "Criando uma Mensagem Personalizada de Congelamento de Dispositivo" na página 331.
6. Sob Ação do Cronômetro, selecione uma das seguintes opções:
   - **Congelar imediatamente**: Depois do período do cronômetro ter decorrido, uma reinicialização ocorre no dispositivo para congelá-lo imediatamente.
   - **Congelar na próxima reinicialização**: Depois do período do cronômetro ter decorrido, o dispositivo é congelado a próxima vez que ele for reiniciado. Esta é a opção padrão.
7. Na área **Opções de Código de Acesso**, selecione uma das seguintes opções:
   - **Gerar um código de acesso aleatório e diferente para cada dispositivo** para gerar automaticamente e utilizar um código de acesso diferente para cada um dos dispositivos de destino.
   - **Gerar o mesmo código de acesso aleatório para cada dispositivo** para gerar automaticamente e usar o mesmo código de acesso para cada um dos dispositivos de destino.
   - **Especifique um código de acesso com 8 dígitos para cada dispositivo** para usar um código de acesso previamente gerado ou personalizado. Clique no campo e insira (ou copie e cole) o código de acesso a usar em cada dispositivo. Para mais informações, consulte "Visualizando o Código de Acesso do Descongelamento" na página 329.
8. Se você desejar atribuir esta política de congelamento de dispositivos do estado offline a cada dispositivo recém-ativado, marque a caixa de seleção adjacente a **Política padrão para dispositivos recém-ativados**.

   Se esta opção está desativada, outra política do estado offline já está definida como a padrão. Para definir esta política como a padrão, você precisa remover esta designação da outra política e depois definir a opção aqui. Para mais informações, consulte "Designando uma Política Padrão do Estado Offline" na página 316.

9. Clique em **Salvar Política** e na caixa de diálogo de Fornecer Autenticação, faça uma das seguintes ações:
   - Se seu método de autenticação de segurança é códigos de autorização enviados por e-mail, digite sua **senha da Central do Cliente** e seu **Código de Autorização**.
   - Se seu método de Autenticação de segurança for tokens RSA SecurID, digite sua **senha da Central do Cliente** e seu **código de token SecurID**.
10. Clique em **OK**. Uma mensagem confirma que a política do estado offline foi criada.
11. Faça uma das seguintes ações, dependendo de se você deseja associar dispositivos à política do estado offline:
    - Se você *não* quiser adicionar dispositivos nesta altura, clique em **Voltar**.

      A página Gerenciar Políticas de Congelamento de Dispositivos se abre. O status da política do estado offline estará definido como Inativo até que a política seja atribuída a um ou mais dispositivos. Para mais informações sobre como adicionar dispositivos a uma política do estado offline, consulte "Adicionando Dispositivos a uma Política do Estado Offline" na página 318.
    - Se desejar adicionar dispositivos à política do estado offline, faça o seguinte:

      i) Se seu método de autenticação de segurança é códigos de autorização enviados por e-mail, você precisa solicitar um segundo código de autorização para adicionar dispositivos à nova política do estado offline. Sob Membros da Política, na área Solicitar Código de Autorização, clique em **Solicitar Código**.

      A Central do Cliente mostra uma mensagem confirmando que um código de autorização foi solicitado e enviado ao endereço de e-mail. Procure a mensagem no seu e-mail.

      ii) Clique em **Adicionar Dispositivos**. Um diálogo se abre.

      iii) No diálogo **Escolher dispositivos para serem adicionados a esta política**, abra a lista **onde o Grupo é** e selecione o grupo de dispositivos certo.

      iv) Se você deseja mostrar dispositivos que cumprem critérios específicos, digite as informações apropriadas nos campos adjacente a **e o campo**.

      v) Por padrão, a lista de dispositivos na grelha de resultados é limitada a apenas aqueles dispositivos que estão elegíveis para atribuição a uma política do estado offline. Se você deseja exibir todos os dispositivos que correspondem aos critérios que você especificou, limpe a caixa de seleção **Mostrar apenas dispositivos elegíveis**.

      NOTA Um dispositivo pode ser associado a apenas uma política do estado offline.

      vi) Selecione os dispositivos que você deseja adicionar:

      - Para selecionar dispositivos individuais, marque a caixa de seleção adjacente a cada dispositivo que deseja adicionar.
      - Para selecionar todos os dispositivos nesta página da tabela, marque a caixa de seleção **Selecionar todos**.

      NOTA É possível alterar o número de registros exibidos por página. Para mais informações, consulte "Alterando o Número de Registros que Aparecem no Relatório" na página 140.

      vii) Clique em **Escolher dispositivo(s)** e na caixa de diálogo de Fornecer Autenticação, faça uma das seguintes ações:

- Se seu método de autenticação de segurança é códigos de autorização enviados por e-mail, digite sua **senha da Central do Cliente** e seu **Código de Autorização**.
- Se seu método de Autenticação de segurança for tokens RSA SecurID, digite sua **senha da Central do Cliente** e seu **código de token SecurID**.

viii) Clique em **OK**.

O diálogo fecha e a grelha de resultados na página Gerenciar Políticas de Congelamento de Dispositivos se atualiza e mostra os dispositivos que você adicionou.

A política é aplicada aos dispositivos adicionados na próxima chamada de agente bem-sucedida. Entretanto, cada status de dispositivo é definido para Atribuição Pendente.

No futuro, se um dispositivo não entrar em contato com o Centro de Monitoramento antes do período do cronômetro ter decorrido, o dispositivo será congelado e uma notificação por e-mail será enviada para o administrador de segurança ou para o usuário de segurança avançado que criou a política do estado offline.

Trabalhando com Políticas do Estado Offline Existentes

É possível usar a página Gerenciar Políticas de Congelamento de Dispositivos do Estado Offline para criar novas políticas do estado offline, ver e editar políticas do estado offline existentes e gerenciar os dispositivos associados a uma política do estado offline.

Para ver a lista de políticas de Congelamento de Dispositivos do estado offline e executar ações nelas:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivos**> **Gerenciar Políticas de Congelamento de Dispositivos do Estado Offline**.

   A página Gerenciar Políticas de Congelamento de Dispositivos do Estado Offline se abre e mostra uma lista de políticas existentes. As seguintes informações aparecem na tabela de cada política:

   - **Nome de Política**: o nome atribuído à política.
   - **Contagem de Dispositivos**: o número de dispositivos associados à política.
   - **Descrição**: uma descrição da política.
   - **Criado por**: o nome de usuário da pessoa que criou a política.
   - **Última Modificação**: a data e hora da última vez que a política foi atualizada.
   - **Status**: o status atual da política do estado offline Os valores possíveis são Ativo e Inativo.

     NOTA Um status de Inativo indica que a política do estado offline foi excluída, mas um ou mais de seus dispositivos associados ainda não chamaram para o Centro de Monitoramento para receber a atualização. Depois de todos os dispositivos fazerem uma chamada de agente, a política é removida do sistema. Para mais informações, consulte "Excluindo uma Política de Congelamento de Dispositivo do Estado Offline" na página 321.

   - **Política Padrão**: só é possível definir uma política como a política padrão. Um valor de Sim indica que a política foi designada como a política padrão a ser atribuida aos dispositivos recém-ativados.

   A partir da página Gerenciar Políticas de Congelamento de Dispositivo do Estado Offline você pode executar as seguintes tarefas se estiver conectado como um administrador de segurança ou usuário de segurança avançado:

- Para procurar uma política do estado offline, insira **Critérios de Pesquisa** e clique em **mostrar resultados**. Para mais informações, consulte "Pesquisando uma Política de Congelamento de Dispositivo do Estado Offline" na página 314.
- Para abrir uma política do estado offline para edição, na grelha de resultados, clique no link para o **Nome da Política**. Para mais informações, consulte "Editando uma Política de Congelamento de Dispositivo do Estado Offline" na página 315.
- Para adicionar ou remover dispositivos, na grelha de resultados, clique no link para o **Nome da Política**. Para mais informações, consulte "Gerenciando Dispositivos Associados a uma Política de Congelamento de Dispositivos do Estado Offline" na página 317.
- Para criar uma nova política do estado offline, clique em **Nova Política**. A página Criar e Editar Política de Congelamento de Dispositivos do Estado Offline se abre. Para mais informações, consulte "Criando uma Política de Congelamento de Dispositivos do Estado Offline" na página 310.
- Para baixar a lista de políticas, clique em . Para mais informações, consulte "Baixando Relatórios" na página 150.
- Para imprimir a página atual da lista de políticas, clique em . Para mais informações, consulte "Imprimindo Relatórios" na página 149.
- Para salvar os filtros que você usou para gerar a lista de políticas, clique em . Para mais informações, consulte "Salvando Filtros de Relatório" na página 149.

Pesquisando uma Política de Congelamento de Dispositivo do Estado Offline

Para pesquisar uma política de congelamento de dispositivos do estado offline:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivos**> **Gerenciar Políticas de Congelamento de Dispositivos do Estado Offline**.
3. Na página Gerenciar Políticas de Congelamento de Dispositivo do Estado Offline, procure a política que você deseja ver usando *qualquer* dos campos dos**Critérios de Pesquisa** da seguinte maneira:
   - No campo **o Nome da Política é ou contém**, digite o nome da política do estado offline.
   - No campo **e a Descrição da Política é ou contém**, insira várias letras que você sabe que estão na descrição do política do estado offline.
   - Clique no campo adjacente a **ou a política contém um dispositivo onde o campo**, selecione o campo apropriado da lista e depois no campo **é ou contém**, use **Escolher** ou digite o valor apropriado para a política do estado offline que deseja ver.
4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e mostra os resultados da pesquisa.

Editando uma Política de Congelamento de Dispositivo do Estado Offline

É possível alterar as configurações de uma política do estado offline em qualquer momento. Se você fizer alterações às configurações do período do cronômetro, mensagem de congelamento ou ação de cronômetro, suas alterações terão efeito nos dispositivos da política do estado offline após a próxima chamada de agente.

NOTA Para alterar os dispositivos associados a uma política do estado offline, consulte "Gerenciando Dispositivos Associados a uma Política de Congelamento de Dispositivos do Estado Offline" na página 317.

Para editar uma política do estado offline:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. Na página Gerenciar Políticas de Congelamento de Dispositivo do Estado Offline, procure a política que você deseja editar. Consulte "Pesquisando uma Política de Congelamento de Dispositivo do Estado Offline" na página 314.
3. Na grelha de resultados, clique no **Nome da Política** da política que deseja editar.
4. Se seu método de autenticação de segurança é o envio de códigos de autenticação de segurança por e-mail, na área Solicitar Código de Autorização, clique em **Solicitar Código**.

   A Central do Cliente mostra uma mensagem confirmando que um código de autorização foi solicitado e enviado ao endereço de e-mail. Procure a mensagem no seu e-mail.
5. Sob Informações da política, edite as seguintes informações, conforme necessário:
   a) Edite o nome no campo **Nome de Política** e clique no link **Verificar a disponibilidade do nome** para verificar se o nome que digitou não está em uso.
   b) Edite a **Descrição da Política**.
   c) No campo **Período do Cronômetro**, edite o número de dias que devem passar antes de um dispositivo ser congelado. Valores entre **4** dias e **365** dias são suportados.
6. Clique no campo **Mensagem de Congelamento** e selecione a mensagem que deseja exibir no dispositivo quando ele é congelado. O texto da mensagem aparece no campo **Visualização da mensagem**.

   Se a mensagem apropriada não existir, clique no link **Criar mensagem** para criar uma nova mensagem. Para mais informações, consulte "Criando uma Mensagem Personalizada de Congelamento de Dispositivo" na página 331.
7. Sob Ação do Cronômetro, selecione uma das seguintes opções:
   - **Congelar imediatamente**: Depois do período do cronômetro ter decorrido, uma reinicialização forçada ocorre no dispositivo para congelá-lo imediatamente.
   - **Congelar na próxima reinicialização**: Depois do período do cronômetro ter decorrido, o dispositivo é congelado a próxima vez que ele for reiniciado. Esta é a opção padrão.
8. Um código de acesso é usado para descongelar o dispositivo congelado. Na área **Opções de Código de Acesso**, selecione uma das seguintes opções:
   - **Gerar um código de acesso aleatório e diferente para cada dispositivo** para gerar automaticamente e utilizar um código de acesso de desbloqueio diferente para cada dispositivo.

- **Gerar o mesmo código de acesso aleatório para cada dispositivo** para gerar e usar o mesmo código de acesso de desbloqueio para cada dispositivo.
- **Especifique um código de acesso com 8 dígitos para cada dispositivo** para usar um código de acesso previamente gerado ou personalizado. Clique no campo e insira (ou copie e cole) o código de acesso a usar em cada dispositivo. Para mais informações, consulte "Visualizando o Código de Acesso do Descongelamento" na página 329.

9. Se você desejar atribuir esta política de congelamento de dispositivos do estado offline a cada dispositivo recém-ativado, marque a caixa de seleção adjacente a **Política padrão para dispositivos recém-ativados**.

 NOTA Se esta opção está desativada, outra política de congelamento de dispositivos do estado offline já está definida como a padrão. Para definir a política que você está editando como a padrão, você precisa remover esta designação da outra política e depois definir a opção aqui. Para mais informações, consulte "Designando uma Política Padrão do Estado Offline" na página 316.

10. Clique em **Salvar Política** e na caixa de diálogo de Fornecer Autenticação, faça uma das seguintes ações:
    - Se seu método de autenticação de segurança é códigos de autorização enviados por e-mail, digite sua **senha da Central do Cliente** e seu **Código de Autorização**.
    - Se seu método de Autenticação de segurança for tokens RSA SecurID, digite sua **senha da Central do Cliente** e seu **código de token SecurID**.
11. Clique em **OK**. Uma mensagem confirma que a política do estado offline foi editada.

    A política do estado offline é atualizada em cada dispositivo na próxima chamada de agente. Entretanto, o status do dispositivo é definido como Atribuição Pendente.

 NOTA Se um dispositivo estiver congelado, a política nesse dispositivo será atualizada após o descongelamento do dispositivo.

Designando uma Política Padrão do Estado Offline

É também possível designar uma política do estado offline como a política padrão a ser atribuída a dispositivos recém-ativadas. Só é possível definir uma política como a política padrão.

Para designar uma política como a política padrão:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivos**> **Gerenciar Políticas de Congelamento de Dispositivos do Estado Offline**.

   A página Gerenciar Políticas de Congelamento de Dispositivos do Estado Offline se abre e mostra uma lista de políticas existentes.
3. Na grelha de resultados, revise os valores na coluna **Política Padrão** para determinar se a política já está definida como a política padrão (valor de coluna está definida como **Sim**).
4. Faça uma das seguintes opções:
   - Se nenhuma política estiver definida como a política padrão, vá para etapa 5.

- Se uma política do estado offline *está* definida como a política padrão e você deseja designar outra política como a padrão, faça o seguinte:
  i) Clique no link **Nome da Política** da política que está atualmente definida como a política padrão.
  ii) Na página Criar uma política de congelamento de dispositivo do estado offline, desmarque a caixa de seleção adjacente a **Política padrão para dispositivos recém-ativados**.
  iii) Clique em **Salvar política**.

5. Clique no link **Nome da Política** da política que você deseja definir como a política padrão.
6. Se seu método de autenticação de segurança é o envio de códigos de autenticação de segurança por e-mail, na área Solicitar Código de Autorização, clique em **Solicitar Código**.

   A Central do Cliente mostra uma mensagem confirmando que um código de autorização foi solicitado e enviado ao endereço de e-mail. Procure a mensagem no seu e-mail.
7. Marque a caixa de seleção adjacente a **Política padrão para dispositivos recém-ativados**.
8. Clique em **Salvar Política** e na caixa de diálogo de Fornecer Autenticação, faça uma das seguintes ações:
   - Se seu método de autenticação de segurança é códigos de autorização enviados por e-mail, digite sua **senha da Central do Cliente** e seu **Código de Autorização**.
   - Se seu método de Autenticação de segurança for tokens RSA SecurID, digite sua **senha da Central do Cliente** e seu **código de token SecurID**.
9. Clique em **OK**.

   Assim que os dispositivos novos forem ativados, a política do estado offline é aplicada em cada dispositivo. No futuro, se um dispositivo não entrar em contato com o Centro de Monitoramento antes do período do cronômetro ter decorrido, o dispositivo será congelado automaticamente e uma notificação por e-mail será enviada para o administrador de segurança ou para o usuário de segurança avançado que criou a política do estado offline.

Gerenciando Dispositivos Associados a uma Política de Congelamento de Dispositivos do Estado Offline

É possível ver os detalhes dos dispositivos de uma política do estado offline. É também possível adicionar dispositivos a uma política do estado offline existente ou remover dispositivos.

NOTA Só é possível associar um dispositivo com uma política do estado offline.

Esta seção descreve as seguintes tarefas:

- Visualizando os Dispositivos Associados a uma Política de Congelamento de Dispositivos do Estado Offline
- Adicionando Dispositivos a uma Política do Estado Offline
- Removendo Dispositivos de uma Política do Estado Offline

Visualizando os Dispositivos Associados a uma Política de Congelamento de Dispositivos do Estado Offline

Para ver os dispositivos associados com uma política do estado offline:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. Na página Gerenciar Políticas de Congelamento de Dispositivos do Estado Offline, procure a política que você deseja ver. Para mais informações, consulte "Pesquisando uma Política de Congelamento de Dispositivo do Estado Offline" na página 314.
3. Na grelha de resultados, clique no link de **Nome da Política** apropriado para abrir a política.
4. Role para a área de Membros da Política. A grelha de resultados mostra os dispositivos associados a esta política.
5. Revise a lista de dispositivos e seus detalhes de dispositivos associados. Um dispositivo pode ter qualquer um dos seguintes status:
   - **Atribuição Pendente**: a política está atribuída ao dispositivo na Central do Cliente, mas o dispositivo ainda não fez uma chamada para o Centro de Monitoramento. Após uma chamada de agente bem-sucedida, a política do estado offline é ativada no dispositivo e o status do dispositivo é atualizado para Atribuído.
   - **Atribuído**: a política do estado offline é implantada no dispositivo e o cronômetro está em andamento.
   - **Atualização Pendente**: a política do estado offline foi editada, mas o dispositivo ainda não fez nenhuma chamada para o Centro de Monitoramento. Após uma chamada de agente bem-sucedida, a política do estado offline é atualizada no dispositivo e o status é atualizado para Atribuído.
   - **Remoção Pendente**: o dispositivo foi removido da política do estado offline, mas o dispositivo ainda não fez nenhuma chamada para o Centro de Monitoramento. Após uma chamada de agente bem-sucedida, o dispositivo é removido da lista de dispositivos associados da política do estado offline na página Gerenciar Políticas de Congelamento de Dispositivo do Estado Offline.
6. Para localizar um dispositivo específico, digite um Identificador, Nome de dispositivo, Nome de usuário ou Número de série no campo de texto e clique em **Filtrar Membros**.
7. Para ordenar a lista por informações específicas, tal como nome de usuário, clique no cabeçalho de coluna apropriado. Para inverter a ordem de classificação, clique no cabeçalho de coluna novamente.

   NOTA Você pode deslocar-se pelas várias páginas da grelha de resultados. Consulte "Deslocando-se Entre as Páginas do Relatório" na página 140.

Adicionando Dispositivos a uma Política do Estado Offline

É possível adicionar dispositivos a uma política do estado offline em qualquer momento. A política é ativada no dispositivo na próxima chamada do agente.

NOTA Só é possível associar um dispositivo com uma política do estado offline.

Para adicionar dispositivos a uma política do estado offline:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. Na página Gerenciar Políticas de Congelamento de Dispositivos do Estado Offline, procure a política a que você deseja adicionar estes dispositivos. Consulte "Pesquisando uma Política de Congelamento de Dispositivo do Estado Offline" na página 314.
3. Na grelha de resultados, clique no link de **Nome da Política** apropriado para abrir a política do estado offline.
4. Se seu método de autenticação de segurança é o envio de códigos de autenticação de segurança por e-mail, sob Membros da Política, na área Solicitar Código de Autorização, clique em **Solicitar Código**.

   A Central do Cliente mostra uma mensagem confirmando que um código de autorização foi solicitado e enviado ao endereço de e-mail. Procure a mensagem no seu e-mail.
5. A grelha de resultados mostra os dispositivos atualmente associados a esta política do estado offline. Clique em **Adicionar Dispositivos**.
6. No diálogo **Escolher dispositivos para serem adicionados a esta política**, abra a lista **onde o Grupo é** e selecione o grupo de dispositivos certo.
7. Se você deseja mostrar dispositivos que cumprem critérios específicos, digite as informações apropriadas nos campos adjacente a **e o campo**.
8. Por padrão, a lista de dispositivos na grelha de resultados é limitada a apenas aqueles dispositivos que estão elegíveis para atribuição a uma política do estado offline. Se você deseja exibir todos os dispositivos que correspondem aos critérios que você especificou, limpe a caixa de seleção **Mostrar apenas dispositivos elegíveis**.
9. Selecione os dispositivos que você deseja adicionar:
   - Para selecionar dispositivos individuais, marque a caixa de seleção adjacente a cada dispositivo que deseja adicionar.
   - Para selecionar todos os dispositivos nesta página da tabela, marque a caixa de seleção **Selecionar todos**.

   NOTA É possível alterar o número de registros exibidos por página. Consulte "Alterando o Número de Registros que Aparecem no Relatório" na página 140.
10. Clique em **Escolher dispositivos** e na caixa de diálogo de Fornecer Autenticação, faça uma das seguintes ações:
    - Se seu método de autenticação de segurança é códigos de autorização enviados por e-mail, digite sua **senha da Central do Cliente** e seu **Código de Autorização**.
    - Se seu método de Autenticação de segurança for tokens RSA SecurID, digite sua **senha da Central do Cliente** e seu **código de token SecurID**.
11. Clique em **OK**.

    O diálogo fecha e a grelha de resultados atualiza-se e mostra os dispositivos que você adicionou. A política do estado offline é atribuída a cada dispositivo na próxima chamada de agente. Entretanto, o status do dispositivo é definido como Atribuição Pendente.

No futuro, se um dispositivo não entrar em contato com o Centro de Monitoramento antes do período do cronômetro ter decorrido, o dispositivo será congelado e uma notificação por e-mail será enviada para o administrador de segurança ou para o usuário de segurança avançado que criou a política do estado offline.

Removendo Dispositivos de uma Política do Estado Offline

Pode ser necessário remover dispositivos de uma política do estado offline. Por exemplo, não é possível executar as seguintes ações em um dispositivo até o dispositivo ser removido de sua política do estado offline:

- Enviar uma solicitação de remoção de agentes
- Enviar um relatório de furto

NOTA Após o dispositivo ser recuperado, é possível adicioná-lo novamente a uma política do estado offline.

NOTA Se um dispositivo for congelado por uma política, ou uma alteração ao seu status for iminente, não é possível remover o dispositivo da política do estado offline.

Para remover dispositivos de uma política do estado offline:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. Na página Gerenciar Políticas de Congelamento de Dispositivo do Estado Offline, procure a política de qual deseja remover dispositivos. Consulte "Pesquisando uma Política de Congelamento de Dispositivo do Estado Offline" na página 314.
3. Na grelha de resultados, clique no link de **Nome da Política** apropriado para abrir a política do estado offline.
4. Role para a área de Membros. A grelha de resultados mostra os dispositivos associados a esta política do estado offline.
5. Selecione os dispositivos que você deseja remover:
   - Para selecionar dispositivos individuais, marque a caixa de seleção adjacente a cada dispositivo que deseja adicionar.
   - Para selecionar todos os dispositivos nesta página da tabela, marque a caixa de seleção **Selecionar todos**.

   NOTA É possível alterar o número de registros exibidos por página. Consulte "Alterando o Número de Registros que Aparecem no Relatório" na página 140.
6. Clique em **Remover Dispositivos Selecionados**.

   Uma mensagem confirma que os dispositivos selecionados foram removidos da política do estado offline, mas a política do estado offline não foi removida do dispositivo até a próxima chamada de agente bem-sucedida. Entretanto, o status do dispositivo é definido como Remoção Pendente.

NOTA Dispositivos que foram removidos de uma política do estado offline não são congelados se estiverem offline durante um período de tempo. Para assegurar que os seus dispositivos gerenciados estejam sempre protegidos, adicione estes dispositivos removidos a uma outra política do estado offline.

Excluindo uma Política de Congelamento de Dispositivo do Estado Offline

Se uma política do estado offline deixou de ser necessária, você pode excluí-la.

Quando você exclui uma política do estado offline o status da política é definido como Inativo enquanto ela aguarda que seus dispositivos faça uma chamada para o Centro de Monitoramento e receba a atualização à política. Depois da política ser removida de todos seus dispositivos, a política é excluída do sistema.

NOTA Os dispositivos que eram associados a uma política excluída não são congelados se estiverem offline durante um período de tempo. Para assegurar que estes dispositivos gerenciados estejam sempre protegidos, adicione estes dispositivos a uma outra política do estado offline. Para mais informações, consulte "Adicionando Dispositivos a uma Política do Estado Offline" na página 318.

Para excluir uma política do estado offline:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. Na página Gerenciar Políticas de Congelamento de Dispositivos do Estado Offline, procure a política que você deseja excluir. Consulte "Pesquisando uma Política de Congelamento de Dispositivo do Estado Offline" na página 314.
3. Na grelha de resultados, clique no link de **Nome da Política** apropriado para abrir a política do estado offline.
4. Clique em **Excluir política**.
5. Na mensagem de confirmação, clique em **Excluir Política**.

   Na página Política de Congelamento de Dispositivos do Estado Offline, o status da política do estado offline altera-se para Inativo e o status de cada dispositivo altera-se para Remoção Pendente.

   Na próxima chamada de agente bem-sucedida a política do estado offline é removida de cada dispositivo. Depois da política ser removida de *todos* os dispositivos da política, a política é excluída do sistema.

   IMPORTANTE A política não pode ser removida de dispositivos com um status de Congelado Por Política. Você precisa descongelar estes dispositivos antes da política poder ser excluída. Para mais informações sobre como descongelar dispositivos congelados, consulte "Descongelando um Dispositivo Congelado" na página 327.

Rastreamento do Status de Congelamento de Dispositivos

A Central do Cliente fornece atualizações de status quase em tempo real sobre o andamento das solicitações de Congelamento de Dispositivo e políticas de Congelamento de Dispositivo do estado offline. O Relatório do Resumo de Congelamento de Dispositivos mostra todos os dispositivos que tiveram uma solicitação de congelamento de dispositivos ou que estão associados a uma política do estado offline. É possível filtrar este relatório por status de Congelamento de Dispositivos para ver dispositivos específicos.

Esta seção oferece informações acerca dos seguintes tópicos:

- Visualizando o Status de Congelamento de Dispositivos
- Visualizando Solicitações de Congelamento de Dispositivo
- Visualizando Dispositivos Congelados por uma Política do Estado Offline

Visualizando o Status de Congelamento de Dispositivos

Para visualizar o status de todas as solicitações de Congelamento de Dispositivos:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Relatório do Resumo de Congelamento de Dispositivo**.
3. Na página Relatório do Resumo de Congelamento de Dispositivos, na área **Critérios de Pesquisa**, defina as opções de filtragem e de exibição preferidas para os resultados, usando um ou mais dos seguintes critérios:
   - Para filtrar os resultados por grupos de dispositivos, no campo **Onde o grupo é**, abra a lista e selecione o grupo de dispositivos desejado.

     NOTA Se você estiver conectado como um usuário de segurança avançado, pode selecionar apenas o Grupo de Dispositivos a que está atribuído.

   - Para filtrar os resultados por **Identificador**, **IMEI**, **Marca**, **Modelo**, ou **Número de Série** específico, no campo **e o** abra a lista e selecione o tipo de valor.

     No campo **é ou contém** digite o valor para ser pesquisado ou use o recurso **Escolher**. Para mais informações sobre o recurso **Escolher**, .consulte "Editando Informações de Ativos" na página 141.
   - Para filtrar por nome de solicitação ou nome de política, no campo **e o Nome de Solicitação/Política é ou contém**, digite o nome completo ou parte do nome.
   - Para filtrar por status, na área **e o status de Congelamento de Dispositivos é**, selecione uma ou mais caixas de seleção a partir destes possíveis valores:
     - **Congelamento Solicitado**: a solicitação foi enviada e está em estado transitório quando aguarda por uma chamada de agente ou quando o processo de configuração de instruções está em execução no dispositivo alvo.
     - **Congelado por Solicitação**: As instruções de Congelamento de Dispositivo foram enviadas ao dispositivo de destino e a mensagem de congelamento é exibida no dispositivo de destino.

- **Descongelamento Solicitado**: instruções para descongelar o dispositivo congelado são enfileiradas e enviadas ao dispositivo na próxima chamada do agente. Este status é geralmente definido quando uma solicitação de descongelamento for definida usando a Central do Cliente.
- **Congelado Por Política**: o dispositivo foi congelado por uma política de Congelamento de Dispositivo do estado offline porque ele não contatou o Centro de Monitoramento antes do período de tempo do cronômetro ter esgotado. A mensagem de congelamento é exibida no dispositivo de destino.
- **Descongelado com Chamada de Agente**: o dispositivo foi descongelado ao enviar uma solicitação de descongelamento na próxima chamada de agente.
- **Solicitação Cancelada**: a solicitação de Congelamento de Dispositivo foi cancelada.
- **Descongelado com Código de Acesso**: o usuário final descongelou o dispositivo ao digitar um **Código de Acesso** no dispositivo congelado.
- **Pendente**:
  - Para solicitações de congelamento de dispositivos, a solicitação está pendente porque a operação de Exclusão de Dados está sendo processada no dispositivo. O dispositivo é congelado após a operação de Exclusão de Dados ser concluída
  - Para políticas do estado offline, a política está pendente porque uma solicitação de Congelamento de Dispositivos foi enviada no dispositivo. Depois da solicitação ser processada, o status altera-se para Política Atribuída.
- **Política Atribuída**: uma política de Congelamento de Dispositivo do estado offline é atribuída ao dispositivo. Se um dispositivo não entrar em contato com o Centro de Monitoramento antes do Período do Cronômetro esgotar, o dispositivo será congelado.
- **Processando**: a solicitação de Congelamento de Dispositivo foi enviada ao dispositivo e está em processamento. Este status é usado para solicitações de congelamento de dispositivos para mais do que um dispositivo.

4. Clique em **Mostrar Resultados** para gerar novamente o relatório usando os critérios especificados.

   O Relatório do Resumo de Congelamento de Dispositivo mostra todos os dispositivos que tiveram uma solicitação de congelamento de dispositivo. Para cada dispositivo listado, o relatório do resumo de congelamento de dispositivos inclui as seguintes informações:

   - **Identificador**: o identificador do dispositivo de destino.
   - **Nome de Solicitação/Política**: o nome atribuído a esta solicitação de Congelamento de Dispositivos ou o nome da política de Congelamento de Dispositivos do estado offline atribuída ao dispositivo
   - **Marca**: a marca do dispositivo de destino
   - **Modelo**: o modelo do dispositivo de destino
   - **N.º de Série**: o número de série do dispositivo de destino
   - **IMEI**: o número de Identificação Internacional de Equipamento Móvel do dispositivo, se aplicável
   - **Solicitado em**: a data e a hora quando a solicitação de Congelamento de Dispositivo foi enviada

- **Período do Cronômetro (dias)**: a duração do período do cronômetro em números de dias. Os valores possíveis são entre 4 e 365 dias. Esta coluna aplica-se apenas àqueles dispositivos que estão associados a uma política de Congelamento de Dispositivos do estado offline.
- **Ação do Cronômetroo**: a ação a ser executada se o período do cronômetro esgotar em um dispositivo. Esta coluna aplica-se apenas àqueles dispositivos que estão associados a uma política de Congelamento de Dispositivos do estado offline.
- **Status**: o status atual da solicitação de congelamento de dispositivo ou da política de congelamento do dispositivo do estado offline.

É possível executar as seguintes tarefas adicionais no relatório gerado, se desejado:

- Para baixar o relatório, clique . Para mais informações, consulte "Baixando Relatórios" na página 150.

NOTA Dependendo do nível de serviço da sua conta, o ícone de download pode não estar disponível.

- Para imprimir a página atual do relatório, clique em . Para mais informações, consulte "Imprimindo Relatórios" na página 149.
- Para salvar os filtros que você usou para gerar o relatório, clique em . Para mais informações, consulte "Salvando Filtros de Relatório" na página 149.

Visualizando Solicitações de Congelamento de Dispositivo

Para visualizar o status e outros detalhes de uma solicitação de Congelamento de Dispositivo:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Relatório do Resumo de Congelamento de Dispositivo**.
3. Na página Relatório do Resumo de Congelamento de Dispositivos digite todos os critérios apropriados para gerar o relatório. Consulte "Visualizando o Status de Congelamento de Dispositivos" na página 322.

   O relatório do resumo do congelamento de dispositivos se atualiza e a grelha de resultados mostra uma lista de todos os dispositivos em sua conta que contêm uma solicitação de congelamento de dispositivo.
4. Faça uma das seguintes ações, dependendo do status da solicitação de Congelamento de Dispositivo:
   - Se o status da solicitação do Congelamento de Dispositivos for **Descongelado** ou **Cancelada**, clique no link **Ver** para abrir a página Detalhes de Congelamento de Dispositivos em um estado de somente leitura para a solicitação selecionada.
   - Se o status da solicitação do Congelamento de Dispositivos for **Congelamento Solicitado**, **Congelado** ou **Pendente**, clique no link **Editar** para abrir a página Detalhes de Congelamento de Dispositivos em um estado editável para a solicitação selecionada.

Visualizando Detalhes sobre uma Solicitação de Congelamento de Dispositivo

A página Detalhes do Congelamento de Dispositivo contém as seguintes informações detalhadas sobre a solicitação de Congelamento de Dispositivo:

- **Status Atual**: o status atual da solicitação de Congelamento de Dispositivo. Os valores possíveis são:
  - **Congelamento Solicitado**: a solicitação foi enviada e está em estado transitório quando aguarda por uma chamada de agente ou quando o processo de configuração de instruções está em execução no dispositivo alvo.
  - **Congelado Por Solicitação**: as instruções de Congelamento do Dispositivo são enviadas ao dispositivo de destino e a mensagem de congelamento é nele exibida.
  - **Descongelamento Solicitado**: instruções para descongelar o dispositivo congelado são enfileiradas e enviadas ao dispositivo na próxima chamada do agente. Este status é geralmente definido quando uma solicitação de descongelamento for definida usando a Central do Cliente.
  - **Descongelado com Chamada de Agente**: o dispositivo foi descongelado ao enviar uma solicitação de descongelamento na próxima chamada de agente.
  - **Descongelado com Código de Acesso**: O usuário final descongelou o dispositivo ao digitar um Código de Acesso no dispositivo congelado
  - **Pendente**: a solicitação está pendente porque a operação de Exclusão de Dados está sendo processada no dispositivo. O dispositivo é congelado após a operação de Exclusão de Dados ser concluída
  - **Processando**: a solicitação de Congelamento de Dispositivo foi enviada ao dispositivo e está em processamento. Este status é usado para solicitações de congelamento de dispositivos para mais do que um dispositivo.
  - **Solicitação Cancelada**: a solicitação de Congelamento de Dispositivo foi cancelada antes de ser implantada no dispositivo de destino.
- **Identificador**: o identificador do dispositivo de destino.
- **IMEI**: o número de Identificação Internacional de Equipamento Móvel do dispositivo, se aplicável
- **Marca**: a marca e fabricante do dispositivo de destino
- **Modelo**: o modelo do dispositivo de destino
- **Número de Série**: o número de série do dispositivo de destino
- **Ativo**: o número de rastreamento de inventário ou de ativo do dispositivo de destino, conforme atribuído pelo administrador da rede na organização
- **Última Chamada**: a data e a hora da última chamada de agente do dispositivo para o Centro de Monitoramento
- **Código de Acesso de Descongelamento**: o código de acesso usado para descongelar o dispositivo manualmente. Para mais informações, consulte "Usando um código de descongelamento no dispositivo de destino" na página 329.
- Tabela de **Status**: as informações detalhadas sobre a atividade de congelamento/descongelamento no dispositivo de destino. As seguintes informações são mostradas:
  - **Etapa**: o número sequencial da alteração do status
  - **Status**: o status da Solicitação de Congelamento
  - **Data**: a data e a hora quando a alteração do status ocorreu

- ○ **Nome de Usuário**: o nome de usuário do administrador de segurança ou usuário de segurança avançado que solicitou a alteração do status

Além destas informações, a página Detalhes do Congelamento de Dispositivo contém os seguintes botões que permitem que você execute tarefas adicionais, tais como:

- **Descongelar dispositivo**: clique para descongelar um dispositivo congelado na próxima chamada do agente. Para mais informações, consulte "Usando a Central do Cliente para Descongelar durante uma Chamada de Agente" na página 327.
- **Cancelar solicitação**: clique para cancelar uma solicitação de Congelamento de Dispositivo antes que o dispositivo seja congelado. Para mais informações, consulte "Gerenciando Mensagens Personalizadas de Congelamento de Dispositivo" na página 331.
- **Remover detalhes**: clique para remover os detalhes de uma Solicitação de Congelamento de Dispositivo. Para mais informações, consulte "Removendo Detalhes de uma Solicitação de Congelamento de Dispositivo" na página 308.

Visualizando Dispositivos Congelados por uma Política do Estado Offline

Quando uma política do estado offline é atribuída a um dispositivo e o dispositivo falha em contatar o Centro de Monitoramento durante um número especificado no período do cronômetro da política do estado offline, o dispositivo é congelado. Administradores recebem uma notificação por e-mail diariamente listando os dispositivos que foram congelados por uma política do estado offline durante as últimas 24 horas.

NOTA Depois de uma notificação por e-mail ser enviada para um dispositivo, nenhum e-mail adicional será enviado, independentemente da quantidade de dias que o dispositivo permanece congelado.

No Relatório do Resumo de Congelamento de Dispositivo, você pode ver uma lista de *todos* os dispositivos que estão atualmente congelados por uma política do estado offline e determinar quais deseja descongelar e quais requerem ações adicionais.

Os dispositivos que são congelados por uma política do estado offline:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Relatório do Resumo de Congelamento de Dispositivo**.
3. No local Critérios de Pesquisa, desmarque as caixas de seleção na área **e o Status de Congelamento de Dispositivos é** exceto **Congelado Por Política**.
4. Clique em **Mostrar Resultados**. A grelha de resultados atualiza-se e mostra apenas aqueles dispositivos que estão congelados porque não contataram o Centro de Monitoramento durante um número de dias especificado no período do cronômetro da sua política.
5. Para ordenar os resultados por Nome de Política, Período do Cronômetro ou Ação do Cronômetro, clique no cabeçalho de coluna apropriado.
6. Para ver os detalhes sobre o dispositivo congelado, clique no link **Editar**. A página Detalhes do Congelamento de Dispositivo se abre e mostra as seguintes informações:
   - **Status Atual**: mostra **Congelado Por Política**, que é o status atual do dispositivo congelado
   - **Identificador**: O Identificador do dispositivo

- **IMEI**:não aplicável a dispositivos do Windows
- **Marca**: a marca e fabricante do dispositivo.
- **Modelo**: o modelo do dispositivo
- **Número de Série**: o número de série do dispositivo
- **Ativo**: o número de rastreamento de inventário ou de ativo do dispositivo, conforme atribuído pelo administrador da rede na organização
- **Última Chamada**: a data e a hora da última chamada de agente do dispositivo para o Centro de Monitoramento.
- **Código de Acesso de Descongelamento**: o código de acesso usado para descongelar o dispositivo manualmente. Para mais informações, consulte "Usando um código de descongelamento no dispositivo de destino" na página 329.
- Tabela de **Status**: as informações detalhadas sobre a atividade de congelamento/descongelamento no dispositivo de destino. As seguintes informações são mostradas:
  - **Etapa**: o número de sequência da alteração do status
  - **Status**: o status da política do estado offline do dispositivo
  - **Data**: a data e a hora quando a alteração do status ocorreu
  - **Nome de Usuário**: o nome de usuário do administrador de segurança ou usuário de segurança avançado que solicitou a alteração do status

Para além destas informações, a página Detalhes de Congelamento de Dispositivo inclui um botão **Descongelar dispositivo** para descongelar o dispositivo congelado na próxima chamada de agente. Para mais informações, consulte "Usando a Central do Cliente para Descongelar durante uma Chamada de Agente" na página 327.

Descongelando um Dispositivo Congelado

Os dispositivos podem ser congelados por uma política de congelamento de dispositivos ou por uma política de congelamento de dispositivos do estado offline. Pessoal de segurança autorizado pode descongelar um dispositivo e torná-lo operacional das duas seguintes maneiras:

- Usando a Central do Cliente para Descongelar durante uma Chamada de Agente
- Usando um código de descongelamento no dispositivo de destino

IMPORTANTE Descongelando um dispositivo força o seu sistema operacional a reiniciar-se.

Usando a Central do Cliente para Descongelar durante uma Chamada de Agente

Pessoal de segurança autorizado pode descongelar um dispositivo usando a página Detalhes do Congelamento de Dispositivo.

NOTA Usuários de segurança Avançado podem descongelar apenas aqueles dispositivos que pertencem ao grupo de dispositivos a que estes usuários foram atribuídos.

Quando a solicitação de descongelamento é definida na Central do Cliente, o dispositivo de destino é descongelado na próxima chamada de agente ao Centro de Monitoramento. Quando um dispositivo é congelado, o agente realiza uma chamada para o Centro de Monitoramento a cada 9 minutos.

IMPORTANTE Dispositivos Android não podem ser descongelados com sucesso usando a Central do Cliente. Para descongelar um dispositivo Android, consulte "Usando um código de descongelamento no dispositivo de destino" na página 329.

Esta seção fornece instruções para as seguintes tarefas:

- Descongelando um Único Dispositivo com uma Chamada De Agente
- Descongelando Vários Dispositivos com Chamadas de Agente

Descongelando um Único Dispositivo com uma Chamada De Agente

Para descongelar um único dispositivo de destino usando a Central do Cliente:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Relatório do Resumo de Congelamento de Dispositivo**.
3. Na página do Relatório do Resumo de Congelamento de Dispositivo, insira todos os critérios desejados e clique em **Mostrar Resultados**. O Relatório do Resumo de Congelamento de Dispositivo se atualiza e mostra uma lista de todos os dispositivos em sua conta que correspondem a seus critérios de pesquisa na grelha de resultados.
4. Para o dispositivo apropriado, clique no link de **Editar**.
5. Na página Detalhes de Congelamento do Dispositivo, clique em **Descongelar Dispositivo**. O dispositivo é descongelado na próxima chamada de agente.

Descongelando Vários Dispositivos com Chamadas de Agente

Para descongelar vários dispositivos ao mesmo tempo usando a Central do Cliente:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Relatório do Resumo de Congelamento de Dispositivo**.
3. Na página Relatório do Resumo de Congelamento de Dispositivo, na área **e o Status de Congelamento do Dispositivo é**, marque a caixa de seleção de **Congelado**.
4. Digite todos os outros critérios desejados nesta página, e depois clique em**Mostrar Resultados**. O Relatório do Resumo de Congelamento de Dispositivo se atualiza e mostra uma lista de todos os dispositivos congelados em sua conta que correspondem a seus critérios de pesquisa na grelha de resultados.
5. Faça uma das seguintes opções:
   - Para selecionar todos os dispositivos exibidos na página atual da grelha de resultados, marque a caixa de seleção no cabeçalho da coluna da extrema esquerda. Todos os dispositivos na página estão selecionados.
   - Para selecionar todos os dispositivos na grelha de resultados, focalize seu mouse sobre a caixa de seleção no cabeçalho da coluna da extrema esquerda e clique em **Selecione a Totalidade (<n>) dos Registros**. Todos os dispositivos no relatório estão selecionados.

6. Clique em **Editar dispositivos selecionados.**
7. Na página Editar Dispositivos Selecionados, na lista de **Ação** para a linha **Congelado**, clique no campo e selecione **Descongelar**.
8. Clique em **Enviar**. O dispositivo é descongelado na próxima chamada de agente.

Usando um código de descongelamento no dispositivo de destino

A maioria dos dispositivos congelados faz uma chamada para o Centro de Monitoramento a cada 9 minutos. Caso o dispositivo não seja capaz de fazer chamadas de agente, é possível descongelá-lo manualmente.

IMPORTANTE O método preferido para o descongelamento de um dispositivo congelado é usar uma chamada de agente. Se possível, é recomendado que os dispositivos sejam descongelados pela definição do status na Central do Cliente. No entanto, caso pretenda descongelar um dispositivo Android, você *deve* usar o método do código de acesso de descongelamento.

Esta seção oferece informações acerca dos seguintes tópicos:

- Visualizando o Código de Acesso do Descongelamento
- Descongelando um Dispositivo com um Código de Acesso

Visualizando o Código de Acesso do Descongelamento

Em certas circunstâncias, não é possível aguardar pela próxima chamada de agente para desbloquear um dispositivo. Em tais casos, é possível descongelar um dispositivo ao digitar um código de acesso no dispositivo congelado. O código de acesso é aleatoriamente gerado quando a solicitação de Congelamento de Dispositivo é criada e é exibido na página Detalhes de Congelamento do Dispositivo.

Para visualizar o código de acesso de descongelamento associado a uma solicitação de Congelamento de Dispositivo:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Relatório do Resumo de Congelamento de Dispositivo**.
3. Na página do Relatório do Resumo de Congelamento de Dispositivo, insira todos os critérios desejados e clique em **Mostrar Resultados**.

   O relatório do resumo do congelamento de dispositivos se atualiza e a grelha de resultados mostra uma lista de todos os dispositivos em sua conta que contêm uma solicitação de congelamento de dispositivo.
4. Clique no link **Editar** para o dispositivo desejado. A página Detalhes do Congelamento de Dispositivo é aberta e mostra os detalhes da solicitação selecionada.
5. Registre o **Código de Acesso de Descongelamento**.
6. Clique em**Descongelar Dispositivo**.

A próxima etapa é de digitar o código de acesso no dispositivo congelado. Para mais informações, consulte "Usando um código de descongelamento no dispositivo de destino" na página 329.

Descongelando um Dispositivo com um Código de Acesso

Para descongelar um dispositivo manualmente:

1. O usuário entra em contato com o Suporte ao Cliente de sua empresa, ou com um Administrador de Segurança ou um Usuário de Segurança Avançado de sua conta, para iniciar uma solicitação de descongelamento manual.
2. O administrador de segurança ou o usuário de segurança avançado gera um código de acesso de descongelamento usando a Central do Cliente e o fornece ao usuário com instruções detalhadas sobre o descongelamento do dispositivo. Para mais informações sobre a solicitação de um código de acesso de descongelamento, consulte "Visualizando o Código de Acesso do Descongelamento" na página 329.
3. O usuário descongela o dispositivo da seguinte forma:
   - Para dispositivos com Windows:
     i) No dispositivo congelado (que não exibe qualquer campo de suporte para facilitar a digitação do código) pressione a tecla de **Esc** no teclado.
     ii) Digite o **Código de Acesso** fornecido usando as teclas numéricas na linha superior do teclado. Se você introduzir o **Código de Acesso** usando o teclado numérico, o Dispositivo congelado não ficará descongelado. O dispositivo é imediatamente descongelado.
   - Para dispositivos Mac:
     i) No dispositivo congelado (que não exibe qualquer campo de suporte para facilitar a digitação do código) pressione a tecla de **Esc** no teclado.
     ii) Digite o **Código de Acesso** fornecido usando as teclas numéricas na linha superior do teclado. Se você introduzir o **Código de Acesso** usando o teclado numérico, o Dispositivo congelado não ficará descongelado.
     iii) Pressione a tecla **Enter** no teclado. O dispositivo é imediatamente descongelado.
   - Para dispositivos móveis:
     i) Ligue o dispositivo congelado.
     ii) Se a mensagem de Congelamento de Dispositivo de tela inteira aparecer, clique em **Desbloquear Agora** na parte inferior da mensagem.
     iii) Na tela de desbloqueio do dispositivo, digite o código de acesso que foi fornecido a você. O dispositivo é imediatamente descongelado.
     iv) Vá para configurações de dispositivos e redefina o código de desbloqueio para o dispositivo.

Gerenciando Mensagens Personalizadas de Congelamento de Dispositivo

Pessoal de segurança autorizado pode criar e editar mensagens personalizadas de Congelamento de Dispositivo, usando uma combinação de texto simples e formatação HTML. Mensagens personalizadas ajudam você garantir que as informações apropriadas estejam disponíveis aos usuários de um dispositivo congelado. Tais mensagens podem incluir informações de contato de suporte e/ou outras informações que sejam necessárias para os usuários ao ligar para o Suporte Global da Absolute Software para restaurar o funcionamento dos dispositivos congelados.

Esta seção fornece instruções para as seguintes tarefas:

- Criando uma Mensagem Personalizada de Congelamento de Dispositivo
- Editando Mensagens Personalizadas de Congelamento de Dispositivo Existentes
- Excluindo Mensagens Personalizadas de Congelamento de Dispositivo Existentes

Criando uma Mensagem Personalizada de Congelamento de Dispositivo

Para criar uma mensagem personalizada de Congelamento de Dispositivo:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Criar Mensagem de Congelamento de Dispositivo**.

   NOTA Alternativamente, você pode também clicar no botão **Adicionar mensagem** na página Gerenciamento de Mensagens de Congelamento de Dispositivo para abrir a página Criar Mensagens de Congelamento de Dispositivo.

3. Na página Criar Mensagem de Congelamento de Dispositivo, no campo **Nome de Mensagem**, digite um título apropriado para a nova mensagem de congelamento do dispositivo. O título é mostrado como uma opção na lista **Selecione uma mensagem** na página Solicitar Congelamento de Dispositivo.
4. No campo **Texto da Mensagem**, digite o texto que você deseja que seja exibido nos dispositivos congelados. É possível usar texto simples ou uma combinação de texto com as seguintes marcas de formatação HTML:
   - <b>: exibir como negrito
   - <i>: texto em itálico
   - <u>: adicionar sublinhado
   - <font>: especifica a fonte para mostrar uma seleção do texto
   - <p>: especifica um parágrafo com espaçamento padrão antes e depois de texto
   -
: adiciona uma quebra de linha sem o espaçamento padrão
5. Clique em **Salvar**. A Central do Cliente salva a nova mensagem e atualiza a página Criar Mensagem de Congelamento de Dispositivo e mostra uma mensagem de confirmação.

Editando Mensagens Personalizadas de Congelamento de Dispositivo Existentes

Para editar mensagens de Congelamento de Dispositivo existentes:

1. Entre na Central do Cliente como um administrador de segurança ou usuário de segurança avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Gerenciar Mensagens de Congelamento de Dispositivo**.

A página Gerenciar Mensagens de Congelamento de Dispositivo é aberta e mostra uma lista de todas as mensagens disponíveis para a sua conta.

3. Clique no **Nome de Mensagem** ou no link **Editar** para a mensagem que deseja editar.
4. Na página Criar Mensagem de Congelamento de Dispositivo, no campo **Texto de Mensagem**, edite a mensagem de forma apropriada.
5. Clique em **Salvar**.

   A Central do Cliente salva a alteração e atualiza a página Criar Mensagem de Congelamento de Dispositivo e mostra uma mensagem de confirmação.

Excluindo Mensagens Personalizadas de Congelamento de Dispositivo Existentes

Para excluir mensagens de Congelamento de Dispositivo existentes:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Congelamento de Dispositivo** > **Gerenciar Mensagens de Congelamento de Dispositivo**.

   A página Gerenciar Mensagens de Congelamento de Dispositivo é aberta e mostra uma lista de todas as mensagens disponíveis para a sua conta.
3. Clique no **Nome de Mensagem** ou no link **Editar** para a mensagem que deseja excluir.
4. Clique em **Excluir**. A Central do Cliente exclui a mensagem e atualiza a página Criar Mensagens de Congelamento de Dispositivo e exibe uma mensagem de confirmação.

Capítulo 13: Usando Recuperação Remota de Arquivos

O recurso Recuperação Remota de Arquivo, permite que administradores de segurança e Usuários de Segurança Avançado recuperem remotamente arquivos que podem conter informações importantes a partir dos dispositivos Windows em sua conta.

Este capítulo fornece informações sobre os seguintes tópicos:

Requisitos Mínimos do Sistema

Recuperação remota de arquivos está disponível para dispositivos que atendam aos seguintes requisitos:

- Sistema operacional Windows: O dispositivo de destino deve ter um dos sistemas operacionais do Windows suportados instalado nele. Consulte "Plataformas Suportadas para o Agente Computrace" na página 22.
- Versão atual do agente Computrace. Consulte "Baixando o Agente Computrace" na página 127.

NOTA O recurso de Recuperação Remota de Arquivos é suportado apenas em dispositivos com Windows.

Antes de começar

Estas são algumas considerações importantes a ter em conta antes de você fazer uma Recuperação Remota de Arquivos, tal como:

- **Dispositivos Furtados**: Você só pode recuperar os arquivos que foram criados antes da data do furto do dispositivo.
- **Caminhos de Arquivo**: Você necessita caminhos de arquivos usando o recurso de Listas de Arquivos para especificar os arquivos a recuperar. Para mais informações, consulte "Usando a Lista de Arquivos" na página 339.
- **Tamanho do Arquivo**: Você pode fazer solicitações de recuperação remota de arquivos para arquivos com menos de 2GB. No entanto, para arquivos maiores que 1GB, as hipóteses de sucesso com a recuperação do arquivo diminuem.
- **Solicitações de Exclusão de Dados em falta**: Você não pode escolher um dispositivo que já tem um pedido de Exclusão de Dados pendente. Você deve ou cancelar a solicitação pendente ou aguardar que a solicitação seja concluída. Para mais informações, consulte "Excluindo ou Cancelando uma Solicitação de Exclusão de Dados" na página 292.
- **Número de Arquivos**: É possível recuperar até 20 arquivos por solicitação.
- **Acessibilidade de arquivos recuperados**: É possível acessar e baixar os arquivos recuperados durante 30 dias depois da recuperação dos arquivos. Depois de 30 dias, os arquivos já não estão disponíveis.

Solicitando a Recuperação Remota de Arquivos

Para solicitar uma Recuperação Remota de Arquivos:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Recuperação Remota de Arquivos** > **Solicitar Recuperação de Arquivo**.
3. Na página Solicitar Recuperação de Arquivo, no campo **Nome da Solicitação**, digite um nome apropriado para a nova solicitação.
4. Na área Selecionar um Dispositivo, clique em **Escolher** para abrir a lista e selecionar o dispositivo desejado.

   Clique no **Identificador** de dispositivo apropriado para selecioná-lo. O diálogo Escolher fecha e a página Solicitar Recuperação de Arquivos se atualiza e mostra o dispositivo selecionado.
5. No campo **Caminho do Arquivo a ser Recuperado**, especifique o caminho do arquivo que você deseja recuperar.
6. Clique em **Adicionar**. O caminho é adicionado à lista de Caminhos de Arquivos.

   Repita para adicionar vários caminhos para a lista.

   NOTA Para remover um caminho da lista, clique em **Remover** correspondente ao caminho que você deseja remover.
7. Leia cuidadosamente o **Aviso Legal** e marque a caixa**Eu aceito** para indicar que você leu o aviso e que aceita os termos e tem a autoridade para executar esta ação.
8. Clique em **Enviar**.

   A solicitação de Recuperação Remota de Arquivos é criada e implantada no dispositivo na próxima chamada do agente.

Visualizando o Status de Recuperação de Arquivos

A Central do Cliente fornece atualizações de status em tempo real sobre o andamento das solicitações de Recuperação Remota de Arquivos. O Relatório do Resumo da Recuperação de Arquivos lista todos os dispositivos para os quais você fez as solicitações.

Para ver o status da Recuperação de Arquivos:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Recuperação Remota de Arquivos** > **Relatório do Resumo da Recuperação de Arquivo**.
3. No Relatório do Resumo da Recuperação de Arquivos, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:
   - Para filtrar os resultados por grupos de dispositivos, no campo **O grupo é**, abra a lista e selecione o grupo de dispositivos desejado.

NOTA Se você estiver conectado como um usuário de segurança avançado, pode selecionar apenas o Grupo de Dispositivos a que está atribuído.

- Para filtrar resultados por dispositivo específico, na área **e o campo** abra a lista e selecione um dos seguintes valores:
  - **Identificador**: Um número de série eletrônico único atribuído ao agente que está instalado em um dispositivo.
  - **Nome de dispositivo**: O nome atribuído ao dispositivo no sistema operacional.
  - **Nome de usuário**: O nome de uma pessoa que está associada a um dispositivo particular.
  - **Marca**: O fabricante de um dispositivo ou outro hardware.
  - **Modelo**: O tipo de produto de um dispositivo ou outro hardware.
- Para filtrar resultados pelo status da Recuperação de Arquivos, na área **e o Status de Recuperação é**, selecione um ou mais dos seguintes valores:
  - **Solicitada**: A solicitação foi enviada e está em estado transitório quando aguarda por uma chamada do agente ou quando o dispositivo de destino está preparando para a operação de recuperação de arquivos.
  - **Recuperando**: A operação de Recuperação de Arquivos está em andamento para recuperar o arquivo solicitado.
  - **Pronto**: A operação de Recuperação de Arquivos terminou de recuperar o arquivo solicitado. O arquivo está pronto para baixar.
  - **Cancelado**: A solicitação de recuperação de arquivo foi cancelada. Para obter mais informações sobre como cancelar uma solicitação de recuperação de arquivos, consulte "Cancelando uma Solicitação de Recuperação de Arquivo" na página 337.
  - **Falhou**: A solicitação de recuperação de arquivos falhou em executar-se no dispositivo de destino.
  - **Descartado**: O arquivo recuperado foi excluído dos servidores.

4. Clique em **Mostrar Resultados**. A grelha de resultados se atualiza e exibe os seguintes dados retornados de acordo com suas escolhas de filtragem.

- **Identificador**: Um número de série eletrônico único atribuído ao agente que está instalado em um dispositivo. Clicando um Identificador exibido na grelha de resultados abre a página do Resumo do Dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
- **Nome de solicitação**: O nome da solicitação da recuperação remota de arquivos.
- **Status**: O status atual da solicitação de Recuperação de Arquivo, que inclui os seguintes valores possíveis:
  - **Solicitada**: A solicitação foi enviada e está em estado transitório quando aguarda por uma chamada do agente ou quando o dispositivo de destino está preparando para a operação de recuperação de arquivos.
  - **Recuperando**: A operação de Recuperação de Arquivos está em andamento para recuperar o arquivo solicitado.
  - **Pronto**: A operação de Recuperação de Arquivos terminou de recuperar o arquivo solicitado. O arquivo está pronto para baixar.

- ○ **Cancelado**: A solicitação de recuperação de arquivo foi cancelada. Para obter mais informações sobre como cancelar uma solicitação de recuperação de arquivos, consulte "Cancelando uma Solicitação de Recuperação de Arquivo" na página 337.
- ○ **Falhou**: A solicitação de recuperação de arquivos falhou em executar-se no dispositivo de destino.
- ○ **Descartado**: O arquivo recuperado foi excluído dos servidores.

- **Ação**: A ação que você pode executar na solicitação
- **Nome do arquivo**: O nome do arquivo recuperado.
- **Tamanho do Arquivo**: O tamanho do arquivo recuperado
- **Nome de dispositivo**: O nome atribuído a este dispositivo no sistema operacional.
- **Nome de usuário**: O nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo
- **Marca**: O fabricante do dispositivo
- **Modelo**: O tipo de produto de um dispositivo ou outro hardware
- **Solicitado em**: A data da solicitação
- **Solicitado por**: O nome do administrador de segurança ou o usuário de segurança avançado que enviou a solicitação.

Baixar arquivos recuperados

Depois de ter criado com sucesso uma solicitação de Recuperação de Arquivos, a solicitação é executada no dispositivo de destino na próxima chamada do agente. Quando a recuperação estiver concluída, você pode baixar os arquivos recuperados para seu dispositivo local.

É possível selecionar um dos seguintes métodos para baixar arquivos recuperados, dependendo do navegador que usa:

- Baixando Arquivos Recuperados Usando o Internet Explorer
- Baixando Arquivos Recuperados Usando o Firefox ou Outro Navegador

Baixando Arquivos Recuperados Usando o Internet Explorer

Para baixar um arquivo usando o Internet Explorer:

1. No separador **Segurança** do diálogo das Opções de Internet, adicione o domínio da Central do Cliente (`cc.absolute.com`) como um site confiável.
2. Para todos os sites confiáveis, clique em **Nível Personalizado** e nas Configurações de Segurança - caixa de diálogo Zona de Sites Confiáveis, ative a opção **Aviso automático para downloads**.
3. Use o Resumo do Relatório de Recuperação de Arquivos para pesquisar a solicitação apropriada. Se o arquivo está disponível para download, a coluna de Status mostra **Pronto**.
4. Na coluna **Nome do Arquivo**, clique no link do nome do arquivo.
5. Digite sua **Senha da Central do Cliente** e seu **Código do Token SecurID** ou **Código de Autorização**. Para mais informações, consulte "Métodos de Autenticação de Segurança" na página 263.
6. Siga as instruções na tela para salvar o arquivo em seu disco rígido local.

Baixando Arquivos Recuperados Usando o Firefox ou Outro Navegador

Para baixar um arquivo usando um navegador diferente do Internet Explorer:

1. Use o Resumo do Relatório de Recuperação de Arquivos para pesquisar a solicitação apropriada. Se o arquivo está disponível para download, a coluna de Status mostra **Pronto**.
2. Na coluna **Nome do Arquivo**, clique no link do nome do arquivo.
3. Digite sua **Senha da Central do Cliente** e seu **Código do Token SecurID** ou **Código de Autorização**. Para mais informações, consulte "Métodos de Autenticação de Segurança" na página 263.
4. Siga as instruções na tela para salvar o arquivo em seu disco rígido local.

Alterando o Status de Recuperação de Arquivos

Dependendo do status atual da Recuperação do Arquivo, é possível fazer uma das seguintes ações:

- Cancelando uma Solicitação de Recuperação de Arquivo
- Removendo Arquivos Recuperados e Arquivos de Registros

A seguinte tabela fornece uma lista de possíveis estados para a Recuperação de Arquivos e as ações que você pode executar para cada um deles.

Estados e Ações Disponíveis para a Recuperação de Arquivos

Status	Ação
Solicitado	**Cancelar**
Recuperando	
Pronto	**Remover**
Cancelado	
Falhou	
Descartado	

Cancelando uma Solicitação de Recuperação de Arquivo

Se o status do processo de recuperação de arquivos está definido como **Solicitado** ou **Em recuperação**, você pode cancelar o pedido e parar a recuperação do arquivo.

Para cancelar uma Solicitação de Recuperação de Arquivos:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Recuperação Remota de Arquivos** > **Relatório do Resumo da Recuperação de Arquivo**.

3. No Relatório do Resumo da Recuperação de Arquivos, no campo **e o Nome de Solicitação é ou contém**, digite o nome de solicitação para pesquisar a solicitação de recuperação de arquivos desejada.

   Se a solicitação de Recuperação de Arquivo ainda não foi executada, ou está atualmente em andamento, a coluna **Status** mostra **Solicitado** ou **Recuperando**.

4. Na coluna**Ação**da solicitação de Recuperação de Arquivo que deseja cancelar, clique no link **Cancelar**.

5. Para cancelar a solicitação, clique em **OK** quando solicitado.

   A página Resumo do Relatório de Recuperação de Arquivo se atualiza e mostra **Cancelado** na coluna **Status** adjacente à solicitação de Recuperação de Arquivo que você cancelou.

Removendo Arquivos Recuperados e Arquivos de Registros

Quando você executar uma solicitação de Recuperação de Arquivos, um arquivo de registro do diretório também é gerado. Este arquivo de registro fornece uma lista de todos os arquivos e seus estados de recuperação.

Quando uma solicitação de Recuperação de Arquivo for bem sucedida, os arquivos que você tinha solicitado estarão disponíveis na Central do Cliente. É possível baixar estes arquivos para uma pasta em seu dispositivo local. Depois que a solicitação de Recuperação de Arquivo estiver completa ou se você cancelar uma solicitação de Recuperação de Arquivos, você pode precisar excluir os arquivos baixados e o arquivo de registro do diretório.

Para remover os arquivos baixados e o arquivo de registro do diretório:

1. Entre na Central do Cliente como um Administrador de Segurança ou Usuário de Segurança Avançado.

2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Recuperação Remota de Arquivos** > **Relatório do Resumo da Recuperação de Arquivo**.

3. Na página Relatório de Resumo de Recuperação de Arquivos, pesquise a solicitação da Recuperação de Arquivos desejada.

   - Se a solicitação de Recuperação de Arquivos estiver concluída e os arquivos estiverem disponíveis para download, a coluna de **Status** mostra **Pronto** e a coluna de **Ação** mostra **Remover**.
   - Se a solicitação de Recuperação de Arquivo não estiver concluída ou for cancelada, a coluna de **Status** exibe a palavra **Falhou** ou **Cancelado** e a coluna de **Ação** exibe a palavra **Remover**.

4. Na coluna **Ação** da solicitação de Recuperação de Arquivo apropriada, clique no link **Remover**.

5. Quando solicitado, se você desejar remover os arquivos recuperados e os arquivos de registro, clique em **OK** para confirmar.

   A página do Resumo do Relatório de Recuperação de Arquivo é atualizada sem nenhum detalhe sobre a solicitação de Recuperação de Arquivo que você acabou de remover.

Capítulo 14: Usando a Lista de Arquivos

O recurso de Lista de Arquivos permite que os administradores de segurança, os administradores e os usuários de segurança avançados da Central do Cliente recuperem remotamente uma lista de arquivos de um dispositivo. É possível usar os caminhos de arquivo completos para fazer solicitações de recuperação remota de arquivos.

As seguintes tarefas estão incluídas nesta seção:

Resumo Geral

Você pode usar a página Solicitação de Lista de Arquivos para enviar uma solicitação para recuperar uma lista de arquivos com extensões específicas disponíveis em um local específico em um dispositivo de destino.

Para facilidade de uso, a Central do Cliente contém uma variedade de extensões de arquivo pré-definidos que você pode recuperar. Se a extensão de arquivo que você deseja não estiver listada na página Solicitação de Listas de Arquivos, você pode também especificar a extensão do arquivo usando a caixa de seleção de **Outro**.

A seguinte tabela fornece uma lista de tipos de arquivo predefinidos que estão disponíveis para você na página Solicitar Lista de Arquivos.

Tipos de Arquivos e de Extensões Pré-definidos

Tipos de Arquivo	Extensões de Arquivo
Arquivos Microsoft Word	*.doc, *.dot
Arquivos Microsoft Excel	*.xls, *.xlt, *.xlam
Arquivos Microsoft Powerpoint	*.ppt, *.pot, *.pps, *.ppam
Arquivos Microsoft Visio	*.vsd, *.vss, *.vst, *.vdx, *.vsx, *.vtx
Arquivos Microsoft Access	*.mar, *.maq, *.mdb, *.accdb, *.accde, *.accdt, *.accd
Arquivos Microsoft Project	*.mpp*. *.mpt*. *.mpx, *.mpd
Arquivos Adobe	*.pdf,*.pm3, *.pm4, *.pm5, *.pm6, *.psd
Arquivos Autocad	*.dwg, *.dxf
Arquivos de Corel Draw	*.cdt
Arquivos de Email Eudora	*.mbx, *.toc
Arquivos de HTML	*.htm
Arquivos de Imagem	*.bmp, *.gif, *.jpg, *.jpeg, *.tif, *.pcx
Arquivos de Planilha de Lotus 1-2-3	*.wk*

Tipos de Arquivos e de Extensões Pré-definidos (continuado)

Tipos de Arquivo	Extensões de Arquivo
Microsoft Office (e outros) Arquivos de Segurança	*.bak
Arquivos Microsoft Outlook	*.pst, *.ost, *.wab
Arquivos de Microsoft Outlook Express	*.dbx
Arquivos de Open Office Writer	*.sdw, *.sxw, *.odt, *.ott
Arquivos de Open Office Calc	*.sdc, *.sxc, *.ods, *.ots
Arquivos de Open Office Impress	*.sdd, *.sxi, *.odp, *.otp
Arquivos de Open Office Draw	*.sda, *.sxd, *.odg, *.otg
Arquivos de Office Base	*.sdb, *.odb
Arquivos de Open Office Math	*.smf, *.sxm, *.odf
Arquivos de Open Office Schedule	*.sds
Arquivos de Paintshop Pro	*.psp, *.ps
Arquivos de Rich-Text	*.rtf
Arquivos de Som	*.mp3, *.wav, *.ogg, *.aif, *.cda, *.rm, *.ram, *.mid, *.m4p
Arquivos de texto	*.txt
Arquivos de Vídeo	*.mov, *.avi, *.mkv, *.mpg, *.mpeg, *.mp4, *.rm, *.ram
Documentos WordPerfect	*.wkb, *.wpd

Requisitos Mínimos do Sistema

A Lista de Arquivos está disponível para dispositivos que atendem aos seguintes requisitos mínimos do sistema:

- Sistemas operacionais Windows: O dispositivo de destino deve ter um dos sistemas operacionais do Windows suportados instalado nele. Consulte "Plataformas Suportadas para o Agente Computrace" na página 22.
- Versão atual do agente Computrace. Consulte "Baixando o Agente Computrace" na página 127.

NOTA O recurso de Lista de Arquivos funciona apenas em dispositivos do Windows com o .NET Framework 2.0 ou superior instalado.

Recuperando uma Lista de Arquivos em Dispositivos Furtados

É possível usar o recurso Lista de Arquivos para fornecer uma lista de arquivos em um dispositivo furtado. No entanto, você só pode recuperar uma lista de arquivos que foram criados antes da data de apresentação do relatório do furto.

Para solicitar uma Lista de Arquivos:

1. Conecte-se à Central do Cliente como um Administrador de Segurança, um Administrador, ou um Usuário de Segurança Avançado.

2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Lista de Arquivos** > **Solicitar Lista de Arquivos**.
3. Na página Solicitar Recuperação de Arquivo, no campo **Nome da Solicitação**, digite um nome apropriado para a nova solicitação.
4. Na área **Selecionar um Dispositivo**, clique em **Escolher** para abrir a lista e selecionar o dispositivo desejado. Clique no **Identificador** de dispositivo apropriado para selecioná-lo. O diálogo Escolher fecha e a página Solicitar Recuperação de Arquivos se atualiza e mostra o dispositivo selecionado.

   NOTA Se você estiver conectado como um usuário de segurança avançado, pode apenas selecionar um dispositivo do Grupo de Dispositivos a que está atribuído.

5. Na área **Selecionar Volume para Verificação**, abra a lista e selecione o volume de onde você deseja recuperar a lista de arquivos.

   NOTA Se você não vir o volume onde seus arquivos estão disponíveis, selecione o volume que você deseja na lista de **Outros**.

6. Recupere os arquivos que deseja de uma das seguintes maneiras:
   - Selecione as caixas de seleção para os arquivos específicos que você deseja recuperar.
   - Especifique um tipo de arquivo que não está incluído na lista de arquivos predefinidos ao marcar a caixa de seleção de **Outros**, localizada no fim da lista, e digitar a extensão de arquivo desejada. Para entradas múltiplas, separe suas escolhas usando vírgulas, tal como**.mov, .avi**.
7. Clique em **Enviar** para criar a solicitação de Lista de Arquivos.

Baixando uma Solicitação de Lista de Arquivos

Para baixar uma lista de arquivos:

1. Conecte-se à Central do Cliente como um Administrador de Segurança, um Administrador, ou um Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Lista de Arquivos** > **Relatório do Resumo de Listas de Arquivos**.
3. Na página Relatório do Resumo de Lista de Arquivos, clique no nome da solicitação.
4. Siga as instruções da tela para salvar o arquivo .txt em seu computador.

Rastreando o Status da Lista de Arquivos

A Central do Cliente fornece atualizações de status em tempo real do andamento das solicitações de Lista de Arquivos. O Relatório do Resumo de Lista de Arquivos fornece uma lista de todos os dispositivos para os quais você fez as solicitações.

Para cada dispositivo listado, a página Relatórios de Resumos de Listas de Arquivos inclui as seguintes informações:

- **Identificador**: Um número de série eletrônico único atribuído ao agente que está instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo do dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
- **Nome da Solicitação**: o nome da solicitação da Lista de Arquivos.
- **Status**: o status atual da solicitação da Lista de Arquivos. Os valores possíveis incluem:
  - **Solicitada**: A solicitação foi enviada e está em estado transitório enquanto aguarda por uma chamada do agente ou enquanto o processo de configuração de instruções está em execução no dispositivo de destino.
  - **Recuperando**: A operação de Lista de Arquivos está em andamento para recuperar a lista a partir do dispositivo solicitado.
  - **Pronto**: A operação de Lista de Arquivos terminou e a lista está pronta para ser baixada.
  - **Cancelado**: A solicitação da Lista de Arquivos foi cancelada.
  - **Falhou**: A solicitação de lista de arquivos falhou em executar-se no dispositivo de destino.
- **Ação**: a ação que você pode executar na solicitação, que inclui as seguintes ações, dependendo do status da solicitação:

<table>
<tr><th>Status</th><th>Ação</th></tr>
<tr><td>Solicitado</td><td rowspan="2">Cancelar</td></tr>
<tr><td>Recuperando</td></tr>
<tr><td>Pronto</td><td rowspan="3">Remover</td></tr>
<tr><td>Cancelado</td></tr>
<tr><td>Falhou</td></tr>
</table>

- **Nome de dispositivo**: O nome atribuído a este dispositivo no sistema operacional.
- **Nome de usuário**: O nome único detectado pelo agente que identifica a pessoa que está associada a este dispositivo
- **Marca**: O fabricante do dispositivo
- **Modelo**: O tipo de produto de um dispositivo ou outro hardware
- **Solicitado em**: a data da solicitação.
- **Nome do Solicitante**: exibe o nome do administrador que enviou a solicitação.

Visualizando o Status de Uma Solicitação de Lista de Arquivos

Para visualizar o status de uma solicitação de Lista de Arquivos:

1. Conecte-se à Central do Cliente como um Administrador de Segurança, um Administrador, ou um Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Lista de Arquivos** > **Relatório do Resumo de Listas de Arquivos**.
3. Na página Relatório de Resumo de Lista de Arquivos, na área **Critérios de Pesquisa**, defina as opções de filtragem e de visualização preferidas para o relatório, usando um ou mais dos seguintes critérios:

- Para filtrar os resultados por grupos de dispositivos, no campo **Onde o grupo é**, abra a lista e selecione o grupo de dispositivos desejado.

  NOTA Se você estiver conectado como um usuário de segurança avançado, pode selecionar apenas o Grupo de Dispositivos a que está atribuído.

- Para filtrar resultados por dispositivo específico, na área **e o campo** abra a lista e selecione um dos seguintes valores:
  - **Identificador**: Um número de série eletrônico único atribuído ao agente que está instalado em um dispositivo. Clique no link para abrir a página Resumo de Dispositivo do dispositivo. Para mais informações, consulte "Editando Informações de Ativos" na página 141.
  - **Nome de dispositivo**: O nome atribuído ao dispositivo no sistema operacional
  - **Nome de usuário**: O nome de uma pessoa que está associada a um dispositivo particular
  - **Marca**: O fabricante de um dispositivo ou outro hardware
  - **Modelo**: O tipo de produto de um dispositivo ou outro hardware
  - **Nome do arquivo**: O nome do arquivo recuperado.
- Para filtrar resultados pelo status da Recuperação de Arquivos, na área **e o Status de Recuperação é**, selecione um ou mais dos seguintes valores:
  - **Solicitada**: A solicitação foi enviada e está em estado transitório enquanto aguarda por uma chamada do agente ou enquanto o processo de configuração de instruções está em execução no dispositivo de destino.
  - **Recuperando**: A operação de Lista de Arquivos está em andamento para recuperar a lista a partir do dispositivo solicitado.
  - **Pronto**: A operação de Lista de Arquivos terminou e a lista está pronta para ser baixada.
  - **Cancelado**: A solicitação da Lista de Arquivos foi cancelada.
  - **Falhou**: A solicitação de lista de arquivos falhou em executar-se no dispositivo de destino.

Alterando o Status de uma Lista de Arquivos

Dependendo do status atual da Lista de Arquivos, é possível fazer uma das seguintes ações:

- Cancelando uma Solicitação de Lista de Arquivos
- Removendo Arquivos Recuperados e Arquivos de Registros

Para uma lista de estados de Listas de Arquivos possíveis e as ações que você pode executar para cada um deles, consulte "Rastreando o Status da Lista de Arquivos" na página 341.

Cancelando uma Solicitação de Lista de Arquivos

Se o status do processo de lista de arquivos está definido como **Solicitado** ou **Recuperando**, você pode cancelar a solicitação e parar a recuperação da lista de arquivos.

Pode cancelar uma solicitação de lista de arquivos:

1. Conecte-se à Central do Cliente como um Administrador de Segurança, um Administrador, ou um Usuário de Segurança Avançado.

2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Lista de Arquivos** > **Relatório do Resumo de Listas de Arquivos**.
3. Na página Relatório de Resumo de Lista de Arquivos, pesquise a solicitação da Lista de Arquivos desejada.

   Se a solicitação de Lista de Arquivos ainda não foi executada ou está atualmente em andamento, a coluna **Status**exibe Solicitado ou Recuperando.
4. Na coluna **Ação** da solicitação de Lista de Arquivos que deseja cancelar, clique no link **Cancelar**.
5. Quando solicitado, se você deseja cancelar a solicitação, clique **OK** para confirmar.

   A página Relatório de Resumo de Lista de Arquivos se atualiza e mostra **Cancelado** na coluna **Status** adjacente à solicitação de Lista de Arquivos que você cancelou.

Removendo Arquivos Recuperados e Arquivos de Registros

Quando você executa uma solicitação de lista de arquivos, um arquivo de registro de diretório é também gerado. Este arquivo de registro fornece uma lista de todos os arquivos e seus estados de recuperação.

Quando uma solicitação de lista de arquivos for bem sucedida, os arquivos que você tinha solicitado estarão disponíveis na Central do Cliente. É possível baixar estas listas de arquivos para uma pasta em seu dispositivo local. Depois que a solicitação de Lista de Arquivos estiver concluída ou se você cancelar uma solicitação de Lista de Arquivos, você pode precisar excluir os arquivos baixados e o arquivo de registro do diretório.

Para remover os arquivos baixados e / ou o arquivo de registro do diretório:

1. Conecte-se à Central do Cliente como um Administrador de Segurança, um Administrador, ou um Usuário de Segurança Avançado.
2. No painel de navegação, clique em **Segurança de Dados e Dispositivos** > **Lista de Arquivos** > **Relatório do Resumo de Listas de Arquivos**.
3. Na página Relatório de Resumo de Lista de Arquivos, pesquise a solicitação da Lista de Arquivos desejada.

   Se a solicitação de Lista de Arquivos tiver sido executada com êxito e os arquivos estiverem disponíveis para baixar, a coluna **Status** exibirá **Pronto** e a coluna **Ação** exibirá **Remover**.

   Se a solicitação de Lista de Arquivos não foi executada ou foi cancelada, a coluna de **Status** exibirá **Falhou** ou **Cancelada** e a coluna de **Ação** exibirá **Remover**.
4. Na coluna de **Ação** da solicitação de Lista de Arquivos apropriada, clique no link **Remover**.
5. Quando solicitado, se você desejar remover a lista de arquivos recuperada e os arquivos de registro, clique em **OK** para confirmar.

   A página Relatório de Resumo de Lista de Arquivos é atualizada sem nenhum detalhe sobre a lista de arquivos que você acabou de remover.

Capítulo 15: Computrace Mobile Theft Management para dispositivos iPad

O serviço de Computrace® Mobile Theft Management (CT MTM) permite que você salvaguarde seus dispositivos iPad e iPad mini em casos de perda ou furto. Este serviço fornece as duas seguintes componentes importantes:

- **Prevenção de perdas para Escolas e Outras Organizações**

  É possível implementar as melhores práticas nas escolas em todo seu distrito escolar ou na sua empresa para certificar que os dispositivos são tratados com responsabilidade. Este programa foca no ensino a estudantes e usuários finais de como evitar se tornar alvos para criminosos ao usar as melhores práticas e ações seguras.

  Uma combinação do uso de processos formais para o relato de dispositivos perdidos ou furtados, do uso de marcas de identidade em dispositivos gerenciados, e o auxílio na percepção do usuário e na aprendizagem pode resultar em uma diminuição da quantidade total de perdas e furtos.

  Para mais informações, consulte o seguinte site:

  www.absolute.com/en/products/mobile-theft-management

- **Investigação de Furto**

  Quando um furto é relatado, a equipe de Investigações da Absolute inicia o serviço de resposta rápida, começa uma investigação para coletar informações e evidências para as autoridades legais, e prepara relatórios investigativos e outros trabalhos críticos para o caso.

  Dependendo do contrato específico de sua empresa com a Absolute Software, o programa de Investigação de Furtos pode incluir uma garantia de serviço caso a equipe não consiga recuperar um dispositivo iPad ou iPad mini.

  Para usar o CT MTM, você deve registrar seus dispositivos iPad e iPad mini na Absolute usando a Central do Cliente. Estas informações, que incluem os números de série dos dispositivos, são críticas para a investigação de um dispositivo furtado pela equipe de Investigação da Absolute.

É possível usar um dos seguintes métodos para gerenciar seus dispositivos usando o CT MTM:

- Gerenciando Seus Dispositivos iPad e iPad mini Manualmente
- Usando um Aplicativo Associado para Recolher Seus Dados de Ativos de iPad (não compatível com iOS 8 ou posterior)

Gerenciando Seus Dispositivos iPad e iPad mini Manualmente

Você pode usar o método manual para importar números de série de dispositivos iPad e iPad mini para a Central do Cliente para inicialmente carregar e manter seus dados de ativos. Usando este método significa que você não escolhe para usar um aplicativo associado para automatizar este processo.

IMPORTANTE Se você usou anteriormente um aplicativo associado para inscrever seus dispositivos iPad e iPad mini compatíveis com iOS 6 e iOS 7 no CT MTM, antes de atualizar qualquer um desses dispositivos para o iOS 8, você deve remover o aplicativo associado de cada dispositivo e reinscrever esses dispositivos usando o método manual.

Você é responsável pela manutenção de sua lista de dispositivos iPad e iPad mini ativos ao carregar os números de série para dispositivos novos e existentes que você deseja inscrever no CT MTM e ao desativar os números de série daqueles dispositivos que pretende remover da lista usando a Central do Cliente.

Usando a Central do Cliente para carregar seus dispositivos iPad e iPad mini inscritos permite-lhe a capacidade de relatar um furto, caso este ocorra. Se você tiver uma Garantia de Serviço, precisa carregar a lista de dispositivos iPad e iPad mini ativos novamente a cada 90 dias.

Empresas podem usar este método manual para gerenciar dispositivos iPad e iPad mini, que inclui as seguintes tarefas:

- Importando Números de Série de iPads para a Central do Cliente
- Removendo Dispositivos iPad e iPad mini do CT MTM
- Relatando o Furto de um Dispositivo iPad Gerenciado Manualmente
- Registrando Seus Dispositivos iPad e iPad mini a cada 90 dias

Importando Números de Série de iPads para a Central do Cliente

Inscrevendo seus dispositivos iPad e iPad mini usando o método manual para o CT MTM requer que você importe sua lista de dispositivos inscritos na Central do Cliente. Empresas com a Garantia de Serviço devem manter sua lista de dispositivos iPad e iPad mini e atualizá-la a cada 90 dias. Consulte "Registrando Seus Dispositivos iPad e iPad mini a cada 90 dias" na página 349.

Para importar os dados de dispositivo de seu iPad e iPad mini:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Dados** > **Importar Dados de Dispositivos CT MTM para Dispositivos iPad**.
3. Na página Importar Dados de Dispositivos CT MTM para Dispositivos iPad, clique em **Ver um arquivo de amostra de dados de dispositivos CT MTM** para abrir o arquivo de amostra. Aumente as colunas para ler como inserir estas informações.
4. Clique em **Abrir** e usando o Microsoft Excel (por exemplo), você pode usar o modelo e inserir seus próprios dados ou pode criar um novo arquivo .csv que contém o **Número de Série de Dispositivo Móvel**, que é obrigatório para cada dispositivo iPad e iPad mini que você deseja registrar.

   É possível também inserir outras informações opcionais que você deseja rastrear com este dispositivo, no entanto, apesar da Central do Cliente armazená-las você não as pode ver sem usar um aplicativo associado.
5. **Salve** este arquivo em seu disco rígido.
6. Na Central do Cliente, na página Importar dados de dispositivos CT MTM para dispositivos iPad, clique em **Navegar** e selecione o arquivo .csv que você criou na etapa 4.
7. Clique em **Carregar Arquivo e Importar Dispositivos CT MTM**.

   Você verá uma mensagem indicando que o upload do arquivo está concluído. Se ocorreu um erro durante o processo de carregamento, você verá uma mensagem com o número de entradas cujo carregamento falhou. Clique no link **Visualizar o arquivo de registros** para ver os erros e depois faça uma revisão ao seu arquivo e carregue-o novamente.

Removendo Dispositivos iPad e iPad mini do CT MTM

Quando você decide que já não quer certos dispositivos iPad e iPad mini inscritos no CT MTM, você pode removê-los e libertar as licenças que usam para outros dispositivos. Empresas que estão usando a Central do Cliente somente para o CT MTM não têm operações de segurança disponíveis e, portanto, não necessitam de um código de autorização.

Você pode usar um dos seguintes métodos para remover dispositivos iPad e iPad mini do CT MTM:

- Interagindo com a Central do Cliente para selecionar dispositivos iPad a serem removidos do CT MTM
- Carregando uma Lista de Dispositivos para Remover Dispositivos iPad de CT MTM

Interagindo com a Central do Cliente para selecionar dispositivos iPad a serem removidos do CT MTM

NOTA Estas instruções se aplicam apenas a empresas que usam a Central do Cliente somente para o CT MTM. Para empresas com operações de segurança de dados e dispositivos, bem como CT MTM, consulte "Interagindo com a Central do Cliente para selecionar dispositivos iPad a serem removidos do CT MTM" na página 355.

Para remover dispositivos iPad e iPad mini inscritos do recurso de CT MTM usando uma solicitação de remoção de agente:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Criar e Visualizar Solicitação de Remoção de Agente**.
3. Na página Criar e Visualizar Solicitações de Remoção de Agentes, clique em **Criar nova solicitação para Remoção do Agente**.
4. No diálogo de Selecionar Dispositivo(s) para Remoção de Agentes, faça o seguinte:
   a) No campo **onde o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado para mostrar uma lista de dispositivos de qual você precisa remover os agentes.
   b) Se você deseja mostrar dispositivos que cumprem critérios específicos, digite as informações apropriadas nos campos adjacente a **e o campo**.

      Por exemplo, você pode querer exibir apenas os dispositivos onde o campo **Nome de Usuário começa com** a palavra **Absolute**.
   c) Por padrão, a lista de dispositivos exibida na grelha de resultados é limitada a apenas aqueles dispositivos a partir dos quais você pode remover o agente. Se você deseja exibir todos os dispositivos que correspondem aos critérios que você especificou, limpe a caixa de seleção **Mostrar apenas dispositivos elegíveis**.
   d) Por padrão, todos os dispositivos que correspondem a seus critérios especificados são mostrados na lista. Se você quer mostrar apenas os dispositivos que estão dormentes, selecione a caixa de seleção **Mostrar Apenas Dispositivos Dormentes**.
   e) Clique em **Filtrar**. A caixa de diálogo Selecionar Dispositivo(s) para Remoção de Agentes é atualizada e mostra uma lista de dispositivos que satisfazem os seus critérios.
   f) Na grelha de resultados, selecione os dispositivos ao fazer uma das seguintes ações na coluna da extrema esquerda, que exibe caixas de seleção:

- Para selecionar dispositivos individuais, marque as caixas de seleção para aqueles dispositivos só.
- Para selecionar todos os dispositivos mostrados apenas nesta página, marque a caixa de seleção no cabeçalho.
- Para selecionar todos os dispositivos que atenderam aos critérios de filtragem, focalize seu mouse sobre a seta na caixa de seleção do cabeçalho. Clique no link **Selecionar todos os registros (<n>)** para selecioná-los todos. A caixa de diálogo Selecionar Dispositivo(s) para Remoção de Agentes é aberta com os dispositivos especificados que você selecionou.

5. Clique em **Continuar** para abrir o diálogo de Definir Dispositivo(s) para Autorização de Remoção de Agentes.
6. Clique em **Definido para remoção**. Uma solicitação de remoção de agentes para os dispositivos que você selecionou é criada e executada nos dispositivos iPad e iPad mini de destino nas suas próximas chamadas de agente.

Para mais informações ou para assistência com esta tarefa, entre em contato com o Suporte Global da Absolute Software (www.absolute.com/en/support).

Carregando uma Lista de Dispositivos para Remover Dispositivos iPad de CT MTM

NOTA Estas instruções se aplicam apenas a empresas que usam a Central do Cliente somente para o CT MTM. Para empresas com operações de segurança de dados e dispositivos, bem como CT MTM, consulte "Carregando uma Lista de Dispositivos para Remover Dispositivos iPad de CT MTM" na página 357.

É provável que você queira remover certos dispositivos iPad e iPad mini do CT MTM e libertar as licenças para outros dispositivos que você deseja registrar.

Você precisa criar um arquivo de texto com os **Identificadores** ou **Números de Série** daqueles dispositivos iPad e iPad mini que você deseja remover do CT MTM e carregar esse arquivo de texto para a Central do Cliente para criar uma solicitação de remoção de agente. Insira a lista de dispositivos iPad e iPad mini a serem removidos em uma única coluna, separando cada entrada com uma linha (pressione `Enter`). Não utilize pontuação nesta lista.

Para carregar este arquivo de texto de dispositivos iPad e iPad mini que você deseja remover do CT MTM ao solicitar uma remoção de agente:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Criar e Visualizar Solicitações de Remoção de Agentes**.
3. Na página Criar e Visualizar Solicitações de Remoção de Agentes, clique em **Carregar lista de dispositivos para Remoção de Agente**.
4. No diálogo Carregar lista de dispositivos para Remoção de Agente, em **Caminho do Arquivo**, clique em **Navegar** para selecioná-lo a partir de seu computador local.
5. Selecione uma das seguintes como o tipo de lista de arquivos:
   - **Identificadores**
   - **Números de Série**

6. Clique em **Carregar Arquivo** e clique em **Definir Para Remoção**, o que removerá o dispositivo da lista de seus dispositivos ativos e libertará a licença deste dispositivo para um outro dispositivo que você pretenda inscrever no CT MTM na sua conta.
7. Você verá uma mensagem para confirmar o upload do arquivo. A mensagem também mostra o número total de entradas e o número total de entradas falhadas, caso existam, no arquivo de texto.

   NOTA Clique em **Ver Arquivo do Registro** para ver o arquivo de registro do último carregamento de arquivos. Alternativamente, você pode acessar o arquivo de registro na página **Meus Relatórios**.

Para mais informações ou para assistência com esta tarefa, entre em contato com a equipe de Serviços Profissionais da Absolute Software em PS-MTM-APP@absolute.com.

Relatando o Furto de um Dispositivo iPad Gerenciado Manualmente

NOTA Para relatar o furto de um dispositivo iPad ou iPad mini gerenciado manualmente, a única informação obrigatória que você deve fornecer é o **Número de série**. É possível fornecer outras informações de identificação que possui também, mas essa informação não aparecerá na Central do Cliente.

Para relatar o furto de um dispositivo iPad ou iPad mini gerenciado manualmente:

1. Use a Central do Cliente para enviar um relatório de furto ao completar as instruções na tarefa, "Relatando um Furto Usando a Central do Cliente" na página 358.

   Uma mensagem de e-mail de resumo é enviada para você, incluindo seu número de caso, contato e outras informações.

   A equipe de Investigações da Absolute trabalham em conjunto com sua autoridade legal local para localizar o dispositivo furtado e uma das seguintes situações ocorrem:

   - Quando o dispositivo é encontrado, a equipe de Investigações da Absolute coordena a devolução do dispositivo a você.
   - Se o dispositivo furtado não for recuperado e você adquiriu uma licença Premium e está elegível para uma garantia de serviço, ela é emitida, mas está sujeita à elegibilidade baseada nos termos do seu Contrato de Serviço do Usuário Final da Absolute
2. Apresente uma queixa oficial junto da sua agência de polícia local. Quando você tem o número do processo policial, envie-o para a equipe de Investigações da Absolute.

Registrando Seus Dispositivos iPad e iPad mini a cada 90 dias

Se você adquiriu uma licença Premium, o registro de sua lista de dispositivos iPad e iPad mini atualmente inscritos no CT MTM a cada 90 dias é um requisito para elegibilidade da Garantia de Serviço. Portanto, a cada 90 dias, você precisa enviar sua lista de dispositivos iPad e iPad mini inscritos novamente, seguindo as instruções fornecidas na tarefa, "Importando Números de Série de iPads para a Central do Cliente" na página 346.

Usando um Aplicativo Associado para Recolher Seus Dados de Ativos de iPad

É possível usar um aplicativo associado para gerenciar seus dispositivos iPad e iPad mini compatíveis com iOS 6 e iOS 7 na Central do Cliente. O objetivo primário de um aplicativo associado é aumentar as chances de recuperar com sucesso seus dispositivos iPad e iPad mini, através de relatórios de furto velozes e usando a disponibilidade de geolocalização. Um aplicativo associado não é um agente Computrace no sentido tradicional. Não é persistente, não fornece informações de relato de software e não consegue executar operações de segurança, tais como a Exclusão de Dados, o Congelamento de Dispositivos, a Recuperação de Arquivos e assim por diante.

IMPORTANTE Para dispositivos iPad e iPad mini que usam iOS 8 ou posterior, você deve usar o método manual de inscrição para tais dispositivos. Para mais informações, consulte Gerenciando Seus Dispositivos iPad e iPad mini Manualmente.

Você pode usar um aplicativo associado para coletar dados de ativos de seus dispositivos iPad e iPad mini compatíveis com iOS 6 e iOS 7 gerenciados e inserir os dados na Central do Cliente, que fornece os seguintes benefícios:

- Um aplicativo associado envia os números de série dos dispositivos à Central do Cliente quando estes são registrados, poupando-lhe a tarefa de carregar manualmente os dados.
- Se ativado, um aplicativo associado envia dados de geolocalização à Central do Cliente para o relato da localização de dispositivos, criando alertas baseados em localização e melhorando a recuperação por furto.
- Dispositivos iPad e iPad mini aparecem junto de seus outros dispositivos gerenciados pelo Computrace em muitos relatórios, tais como o Relatório de Ativos, o Resumo do Dispositivo e o Relatório de Dispositivos Móveis. É provável que você queira considerar a criação de um Grupo de Dispositivos para todos seus dispositivos iPad e iPad mini para que possa filtrar e executar relatórios para esses dispositivos específicos apenas. Para mais informações, consulte "Criando um Novo Grupo de Dispositivos" na página 79.
- Com um aplicativo associado implantado, você pode usar a funcionalidade de relatórios de furto da Central do Cliente para relatar um furto de um dispositivo iPad ou iPad mini gerenciado sem primeiro ter um relatório policial registrado. Ao fazê-lo assim, a Equipe de Investigação da Absolute começa imediatamente com a recuperação, enquanto você relata o furto e trata da papelada junto de sua autoridade legal local.

Criando um aplicativo associado personalizado é simples, como descrito na seguinte visão geral de alto nível:

- Trate dos pré-requisitos, tal como solicitar uma conta do iOS Developer Enterprise Program (iDEP) da Apple para que você possa compilar, assinar e implantar aplicativos internos. Para mais informações, vá para a seguinte página Web: https://developer.apple.com/programs/ios/enterprise/.
- Baixe o software development kit (SDK) CT MTM para iPad da Central do Cliente, depois crie e assine digitalmente um aplicativo associado com seu certificado de autenticação para produzir um aplicativo associado personalizado para sua empresa. Para informações sobre como baixar o CT MTM SDK, assiná-lo e implantar um aplicativo associado em seus dispositivos iPad e iPad mini, consulte "Baixando o CT MTM SDK" na página 352.

- Planeie e verifique a implantação de seu aplicativo associado para os dispositivos iPad e iPad mini de sua empresa.

Esta seção fornece as seguintes informações e tarefas:

- Importando Dados de Dispositivos iPad para a Central do Cliente.
- Criando um Aplicativo Associado
- Criando Alertas para Dispositivos iPad e iPad mini
- Removendo o Aplicativo Associado em Dispositivos iPad e iPad mini
- Relatando um Furto Usando a Central do Cliente

Importando Dados de Dispositivos iPad para a Central do Cliente.

Você consegue integrar uma associação de dados melhorada entre seus dispositivos iPad e iPad mini compatíveis com iOS 6 e iOS 7 com CT MTM ao importar os dados para sua conta na Central do Cliente. A Central do Cliente fornece um modelo de amostra para mostrar a você como inserir as informações no arquivo .csv e para você usar para importar seus dados. Leia a seguinte tarefa até ao fim antes de tentar começar a ficar com uma ideia clara daquilo que você necessita fazer e do que está disponível para ajudá-lo com este processo.

Para importar os dados dos seus dispositivos iPad e iPad mini compatíveis com iOS 6 e iOS 7 para a Central do Cliente:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Dados** > **Importar Dados de Dispositivos CT MTM para Dispositivos iPad**.
3. Na página Importar Dados de Dispositivos CT MTM para Dispositivos iPad, clique em **Ver um arquivo de amostra de dados de dispositivos CT MTM** para localizar o arquivo de amostra. Aumente as colunas para ler a ordem em que estas informações devem ser inseridas.
4. Clique em **Abrir** e usando o Microsoft Excel (por exemplo), você pode usar o modelo e inserir seus próprios dados ou pode criar um novo arquivo .csv que contém as seguintes informações para cada dispositivo iPad e iPad mini que você deseja gerenciar:
   - Informações obrigatórias necessárias: **Número de Série de Dispositivo Móvel**
   - Informações opcionais, que aparecem apenas se você está usando um aplicativo associado, inclui:
     - **Endereço MAC Wi-Fi de Dispositivo Móvel**
     - **IMEI/MEID de Dispositivo Móvel**
     - **Número de Telefone de Dispositivo Móvel**
     - **Tecnologia Celular de Dispositivo Móvel**

   Salve este arquivo em seu disco rígido.
5. Na Central do Cliente, na página Importar dados de dispositivos CT MTM para dispositivos iPad, clique em **Navegar** e selecione o arquivo .csv que você criou na etapa 4. Clique em **Abrir**.
6. Clique em **Carregar Arquivo e Importar Dispositivos CT MTM**.

Você verá uma barra de status que mostra o progresso de sua solicitação e depois uma mensagem que informa que o carregamento do arquivo foi concluído. Se ocorreu um erro durante o processo de carregamento, você verá uma mensagem com o número de entradas cujo carregamento falhou. Clique no link **Visualizar o arquivo de registros** para ver os erros e depois faça uma revisão ao seu arquivo e carregue-o novamente.

Para ver todos os arquivos .csv importados e seus registros para aplicativos associados, clique em **Meus Relatórios** e depois clique no link **Pronto** no lado direito do aplicativo associado apropriado.

Criando um Aplicativo Associado

Antes de você poder criar um aplicativo associado, precisa de uma conta do iOS Developer Enterprise Program da Apple para que possa criar aplicativos "internos", tais como o aplicativo associado e prepará-los para serem implantados em seus dispositivos iPad e iPad mini.

Depois de criar um aplicativo associado, você pode carregá-lo para a Central do Cliente para disponibilizá-lo para uso futuro ou para outros administradores da Central do Cliente na sua empresa.

Esta seção fornece informação sobre as seguintes tarefas:

- Baixando o CT MTM SDK
- Carregando um Novo Aplicativo Associado
- Usando um Aplicativo Associado Existente
- Substituindo um Aplicativo Associado Existente
- Excluindo um Aplicativo Associado

Baixando o CT MTM SDK

A primeira vez que você deseja criar um aplicativo associado e para quaisquer novos aplicativos associados que você deseja criar, você precisa executar a seguinte tarefa.

Para baixar o CT MTM SDK para iPad para compilar um aplicativo associado pela primeira vez:

1. Entre na Central do Cliente como um Administrador.
2. Role para baixo na Home page e na área **Links Úteis**, clique no link **Baixar Pacotes**.
3. Role para baixo na página Baixar Pacotes para o local de CT MTM SDK e clique no link **Baixar CT MTM SDK**.

   A Central do Cliente cria um SDK configurado para sua conta. No diálogo na parte inferior da página, clique **Salvar Como** para salvar o arquivo zip no local que deseja.
4. Você deve agora autenticar com código o SDK com o certificado de autenticação iDEP de sua empresa para criar o aplicativo associado.
5. Implante este aplicativo associado em seus dispositivos usando uma das seguintes ferramentas de gerenciamento de ativos:
   - Crie um aplicativo do Enterprise Computrace (CT) para aplicativos iOS no Absolute Manage e depois implante o aplicativo em um iPad ou iPad mini com o Absolute Manage MDM usando um dos seguintes métodos:
     - Instalação Direta
     - Arrastar e soltar usando uma política
     - Auto-instalação usando uma política

- Configurador Apple
- Outras ferramentas MDM de terceiros
- Direto no iTunes

IMPORTANTE Você precisa instalar e iniciar este aplicativo associado em seus dispositivos iPad e iPad mini.

Para mais informações ou para assistência com esta tarefa, entre em contato com a equipe de Serviços Profissionais da Absolute Software em (PS-MRM-APP@absolute.com).

Carregando um Novo Aplicativo Associado

Quando o CT MTM SDK é assinado por código com seu certificado assinado, você pode então criar um aplicativo associado.

Para carregar um novo aplicativo associado:

1. Entre na Central do Cliente como um Administrador.
2. Role para baixo na Home page e na área **Links Úteis**, clique no link **Baixar Pacotes**.
3. Role para baixo na página Baixar Pacotes para a área do **Aplicativo Associado**, clique em **Navegar** e vá para o local onde seu aplicativo associado (arquivo .ipa) está armazenado.
4. Selecione o aplicativo associado desejado.
5. Com o **Nome do arquivo** nesse campo, clique em **Carregar**.

Usando um Aplicativo Associado Existente

Para usar um aplicativo associado existente:

1. Entre na Central do Cliente como um Administrador.
2. Role para baixo na Home page e na área **Links Úteis**, clique no link **Baixar Pacotes**.
3. Role para baixo na página Baixar Pacotes para a área do **Aplicativo Associado** e use um aplicativo associado existente que foi carregado anteriormente ao selecionar o apropriado da lista.
4. Salve o aplicativo associado e envie-o por push para um dispositivo iPad e iPad mini usando uma ferramenta de gerenciamento de ativos descrita na etapa 5 da tarefa, "Baixando o CT MTM SDK" na página 352.

Substituindo um Aplicativo Associado Existente

Pode haver alturas quando você deseja sobrescrever uma versão anterior salva de um aplicativo associado com uma versão nova.

Para sobrescrever um aplicativo associado existente com uma versão mais recente dela:

1. Entre na Central do Cliente como um Administrador.
2. Role para baixo na Home page e na área **Links Úteis**, clique no link **Baixar Pacotes**.

3. Role para baixo na página Baixar Pacotes para a área do **Aplicativo Associado** e clique em **Navegar** para ir para o local onde seu aplicativo associado (arquivo .ipa) está armazenado.
4. Selecione o aplicativo associado desejado que você deseja substituir e clique em **Abrir**.
5. Com o **Nome do arquivo** preenchido nesse campo, clique em **Carregar**.
6. No diálogo uma mensagem mostra o nome do arquivo e pede a você para confirmar. Clique em **OK** para substituir o arquivo mais antigo com a versão mais nova. Estes nomes de arquivos deve ser exatamente iguais. Você verá uma mensagem indicando que o upload foi bem-sucedido.

Excluindo um Aplicativo Associado

Você pode decidir não manter versões anteriores salvas de um aplicativo associado por uma razão ou outra. Portanto, você pode excluir versões mais antigas e obsoletas de seus aplicativos associados.

Para excluir um aplicativo associado:

1. Entre na Central do Cliente como um Administrador.
2. Role para baixo na Home page e na área **Links Úteis**, clique no link **Baixar Pacotes**.
3. Role para baixo na página Baixar Pacotes para a área do **Aplicativo Associado** e, na lista, coloque seu cursor na linha com o aplicativo associado que você pretende excluir e clique em **Excluir**.
4. No diálogo de validação, clique em **OK** para excluir este aplicativo associado.

Criando Alertas para Dispositivos iPad e iPad mini

Se você tiver uma Garantia de Serviço, para esta garantia estar em vigor, os dispositivos precisam realizar chamadas regularmente. Para mais informações, consulte seu Contrato de Serviço do Usuário Final. Você pode rastrear seus dispositivos iPad e iPad mini ao definir alertas e executar relatórios, da seguinte forma:

- Você pode criar um alerta para dispositivos iPad e iPad mini que não chamaram para o Centro de Monitoramento durante um certo período de tempo. Consulte "Criando Novos Alertas Personalizados" na página 43.
- Você pode executar um relatório de dispositivos em falta para ver quais os dispositivos que não estão realizando chamadas. Consulte "Relatório de Dispositivos em Falta" na página 210.
- Quando você ativa a opção de geolocalização para seus dispositivos iPad e iPad mini, pode configurar uma cerca geográfica para alertá-lo quando o dispositivo se desloca para fora de seus limites.Consulte "Criando um Alerta de Cerca Geográfica" na página 45.

Para mais informações sobre alertas, consulte "Gerenciando Alertas" na página 47.

Removendo o Aplicativo Associado em Dispositivos iPad e iPad mini

Quando você decide que já não quer certos dispositivos iPad e iPad mini compatíveis com iOS 6 e iOS 7 inscritos no CT MTM, você pode desativá-los e libertar as licenças que usam para outros dispositivos iPad e iPad mini. Você deve ter tratado dos seguintes pré-requisitos antes de poder continuar com esta tarefa:

- A Absolute Software deve ter um acordo de pré-autorização assinado por sua empresa nos seus registros. Este contrato é um pré-requisito para sua empresa receber uma conta da Central do Cliente. Sua conta indica à Central do Cliente que operações de segurança estão disponíveis para sua empresa.

  Para acessar o formulário do acordo de autorização:

  a) No painel de navegação, clique em **Documentação**.

  b) Na página Documentação, role para **Formulários de Solicitação de Serviço** e clique em **Formulário da Autorização de Administração de Segurança e da Geolocalização** para abrir o formulário.

- Um Nome de Usuário da Central do Cliente e uma Senha associadada que fornecem privilégios de Administrador de Segurança ou de Usuário de Segurança Avançado. Para mais informações, consulte "Funções de usuário e seus direitos de acesso" na página 96.
- Um código de autorização gerado pelo seu token RSA SecurID ou recebido da Central do Cliente em uma mensagem de e-mail, conforme o método de autenticação aplicável. Cada operação de segurança deve ser fundamentada usando um código de autorização disponível apenas ao administrador de segurança que está solicitando o serviço de segurança. Para mais informações, consulte "Métodos de Autenticação de Segurança" na página 263.
- O administrador de segurança de sua empresa atribuiu a capacidade de solicitar a remoção de agentes a um ou mais administradores ou usuários avançados.

  Para informações sobre a concessão do privilégio da Solicitação de Remoção de Agente a administradores e usuários avançados, consulte "Criar Novos Usuários" na página 108. Para informações sobre como criar solicitações de remoção de agentes, consulte "Gerenciando solicitações de remoção de agentes" na página 132.

É possível usar um dos seguintes métodos para remover dispositivos iPad e iPad mini compatíveis com iOS 6 e iOS 7 do CT MTM:

- Interagindo com a Central do Cliente para selecionar dispositivos iPad a serem removidos do CT MTM
- Carregando uma Lista de Dispositivos para Remover Dispositivos iPad de CT MTM

Interagindo com a Central do Cliente para selecionar dispositivos iPad a serem removidos do CT MTM

Para remover dispositivos iPad e iPad mini compatíveis com iOS 6 e iOS 7 inscritos do recurso de CT MTM usando uma solicitação de remoção de agente:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Administração** > **Conta** > **Criar e Visualizar Solicitação de Remoção de Agente**.
3. Na página Criar e Visualizar Solicitações de Remoção de Agentes, clique em **Criar nova solicitação para Remoção do Agente**.

4. No diálogo de Selecionar Dispositivo(s) para Remoção de Agentes, faça o seguinte:
    a) No campo **onde o Grupo é**, abra a lista e selecione o grupo de dispositivos desejado para mostrar uma lista de dispositivos de qual você precisa remover os agentes.
    b) Se você deseja mostrar dispositivos que cumprem critérios específicos, digite as informações apropriadas nos campos adjacente a **e o campo**.

        Por exemplo, você pode querer exibir apenas os dispositivos onde o campo **Nome de Usuário começa com** a palavra **Absolute**.
    c) Por padrão, a lista de dispositivos exibida na grelha de resultados é limitada a apenas aqueles dispositivos a partir dos quais você pode remover o agente. Se você deseja exibir todos os dispositivos que correspondem aos critérios que você especificou, limpe a caixa de seleção **Mostrar apenas dispositivos elegíveis**.
    d) Por padrão, todos os dispositivos que correspondem a seus critérios especificados são mostrados na lista. Se você quer mostrar apenas os dispositivos que estão dormentes, selecione a caixa de seleção **Mostrar Apenas Dispositivos Dormentes**.
    e) Clique em **Filtrar**. A caixa de diálogo Selecionar Dispositivo(s) para Remoção de Agentes é atualizada e mostra uma lista de dispositivos que satisfazem os seus critérios.
    f) Na grelha de resultados, selecione os dispositivos ao fazer uma das seguintes ações na coluna da extrema esquerda, que exibe caixas de seleção:
        - Para selecionar dispositivos individuais, clique nas caixas de seleção individuais para aqueles dispositivos só.
        - Para selecionar todos os dispositivos mostrados apenas nesta página, marque a caixa de seleção no cabeçalho.
        - Para selecionar todos os dispositivos que atenderam aos critérios de filtragem, focalize seu mouse sobre a seta na caixa de seleção do cabeçalho. Clique no link **Selecionar todos os registros (<n>)** para selecioná-los todos. A caixa de diálogo Selecionar Dispositivo(s) para Remoção de Agentes é aberta com os dispositivos especificados que você selecionou.
5. Clique em **Continuar** para abrir o diálogo de Definir Dispositivo(s) para Autorização de Remoção de Agentes.
6. Os administradores de segurança são solicitados a fornecer autorização. Dependendo do método de autenticação de segurança sua empresa escolheu, faça uma das seguintes ações:
    - Para empresas que usam tokens RSA SecurID para serviços de segurança, digite sua **Senha da Central do Cliente** e seu **Código do Token SecurID**.

        Para mais informações, consulte "Usando Tokens RSA SecurID para Serviços de Segurança" na página 263.
    - Para empresas que usam códigos de autorização enviados por e-mail para serviços de segurança:
        i) Clique em **Solicitar Código de Autorização**. A página se atualiza e fornece confirmação de que uma mensagem de e-mail foi enviada para o endereço registrado para o administrador de segurança que está fazendo a solicitação.
        ii) Digite sua **Senha da Central do Cliente** e seu **Código de Autorização**.

        Para mais informações, consulte "Usando Códigos de Autorização Enviados por E-mail para Serviços de Segurança" na página 264.

7. Clique em **Definido para remoção**. Uma solicitação de remoção de agentes para os dispositivos que você selecionou é criada e executada nos dispositivos iPad e iPad mini de destino nas suas próximas chamadas de agente.

Carregando uma Lista de Dispositivos para Remover Dispositivos iPad de CT MTM

É provável que você queira remover certos dispositivos iPad e iPad mini compatíveis com iOS 6 e iOS 7 do CT MTM e libertar as licenças que esses dispositivos usam para outros dispositivos iPad e iPad mini que você deseja registrar.

Você precisa criar um arquivo de texto com os **Identificadores** ou **Números de Série** daqueles dispositivos iPad que você deseja remover do CT MTM e carregar esse arquivo de texto para a Central do Cliente para criar uma solicitação de remoção de agente. Insira a lista de dispositivos iPad e iPad mini a serem removidos em uma única coluna, separando cada entrada com uma linha (pressione **Enter**). Não utilize pontuação nesta lista.

Para carregar este arquivo de texto de dispositivos iPad e iPad mini compatíveis com iOS 6 e iOS 7 que você deseja remover do CT MTM ao solicitar uma remoção de agente:

1. Acesse a Central do Cliente usando o URL específico de sua empresa e se conecte como um usuário de segurança com privilégios.
2. No painel de navegação, clique em **Administração** > **Conta** > **Criar e Visualizar Solicitações de Remoção de Agentes**.
3. Na página Criar e Visualizar Solicitações de Remoção de Agentes, clique em **Carregar lista de dispositivos para Remoção de Agente**.
4. No diálogo Carregar lista de dispositivos para Remoção de Agente, em **Caminho do Arquivo**, clique em **Navegar** para selecionar o arquivo a partir de seu computador local.
5. Selecione uma das seguintes como o tipo de lista de arquivos:
   - **Identificadores**
   - **Números de Série**
6. Clique em **Carregar Arquivo**.

   Você é solicitado a fornecer autorização. Dependendo do método de autenticação de segurança sua empresa escolheu, faça uma das seguintes ações:
   - Para empresas que usam tokens RSA SecurID para serviços de segurança, digite sua **Senha da Central do Cliente** e seu **Código do Token SecurID**.

     Para mais informações, consulte "Usando Tokens RSA SecurID para Serviços de Segurança" na página 263.
   - Para empresas que usam códigos de autorização enviados por e-mail para serviços de segurança:
     i) Clique em **Solicitar Código de Autorização**. A página se atualiza e fornece confirmação de que uma mensagem de e-mail foi enviada para o endereço registrado para o administrador de segurança que está fazendo a solicitação.
     ii) Digite sua **Senha da Central do Cliente** e seu **Código de Autorização**.

     Para mais informações, consulte "Usando Códigos de Autorização Enviados por E-mail para Serviços de Segurança" na página 264.

7. Clique em **Definir Para Remoção**, que removerá o dispositivo da lista de seus dispositivos ativos e libertará a licença deste dispositivo para um outro dispositivo iPad ou iPad mini que você pretenda inscrever na sua conta do CT MTM.

   Você verá uma mensagem para confirmar o upload do arquivo. A mensagem também mostra o número total de entradas e o número total de entradas falhadas, caso existam, no arquivo de texto.

   NOTA Clique em **Ver Arquivo do Registro** para ver o arquivo de registro do último carregamento de arquivos. Alternativamente, você pode acessar o arquivo de registro na página **Meus Relatórios**.

Para mais informações ou para assistência com esta tarefa, entre em contato com o Suporte Global da Absolute Software em www.absolute.com/en/support.

Relatando um Furto Usando a Central do Cliente

Você pode usar a funcionalidade de relatórios de furto da Central do Cliente para relatar o furto de um dispositivo iPad ou iPad mini compatível com iOS 6 e iOS 7 gerenciado sem primeiro ter que completar um relatório policial. Ao fazê-lo assim, a Equipe de Investigação da Absolute começa imediatamente com a recuperação, enquanto você relata o furto e trata da papelada junto de sua autoridade legal local. Para mais informações sobre o Relato de Furtos, consulte "Relatando o Furto de um Dispositivo Gerenciado" na página 377.

Para criar um Relatório de Furto para um dispositivo iPad ou iPad mini compatível com iOS 6 e iOS 7 que foi furtado:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique **Relatório de Furto**.
3. Na página Relatórios de Furto ou no painel de navegação, faça uma das seguintes ações para abrir a página Criar e Editar Relatórios de Furto:
   - Clique no link **Criar e Editar Relatórios de Furto**.
   - Clique em **Resumo de Relatórios de Furto** e na página Resumos de Relatórios de Furto, entre os locais de grelha de **Critérios de Pesquisa** e resultados, clique em **Criar relatório de furto**.
4. Na área **Que dispositivo?**, no campo **Escolher Dispositivo**, clique em **Escolher** para abrir o diálogo de Escolher o Identificador onde você clica no registro apropriado em uma lista de todos os dispositivos detectados para selecioná-lo. Para mais informações sobre o recurso **Escolher**, .consulte "Editando Informações de Ativos" na página 141.

   O diálogo Escolher Identificador se fecha e a página Criar e Editar Relatórios de Furto se atualiza e preenche os campos **Marca**, **Modelo**, **Número de Série**, **Número de Ativo**, e **Sistema Operacional**.
5. Na área **Como é que o dispositivo foi furtado?**, faça o seguinte:

   IMPORTANTE Quanto mais precisas e detalhadas forem as informações fornecidas, maior a probabilidade de que a polícia possa ajudar a facilitar a recuperação. Os campos obrigatórios são indicados por um asterisco (*).

- Nos campos **Data e Hora do Furto**, digite a **data** (formato dd/mm/aaaa) no primeiro campo ou abra o calendário e selecione a data desejada. No segundo campo, digite a **hora** no formato hh:mm.
- No campo **Fuso Horário**, abra a lista e selecione o Fuso Horário desejado.
- Nos campos de **Local do Furto**, insira o endereço completo onde o furto aconteceu.
- No campo **Nome da Vítima**,digite o nome completo da vítima.
- Nos campo de **Cidade do Furto**, insira a cidade ou vila onde o furto aconteceu.
- No campo **País de Furto**, abra a lista e selecione o país onde o furto aconteceu.
- No campo **Estado/Província do Furto**, insira o estado ou a província onde o furto aconteceu.
- Nas opções de **O cabo de alimentação foi furtado?**, clique na resposta desejada a partir de **Sim**, **Não**, e **Desconhecida**.
- No campo **Detalhes do Furto**, insira os detalhes acerca da última localização conhecida do dispositivo e como o mesmo foi furtado.

6. Na área de **Você já registrou uma ocorrência junto à polícia?**, insira a seguinte informação usando o relatório da polícia que você preencheu quando relatou o furto às autoridades.

IMPORTANTE Se você selecionou um dispositivo iPad ou iPad mini na etapa 4, a Central do Cliente sabe que você não tem de registrar uma ocorrência policial ou inserir esta informação antes de enviar um Relatório de Furto. Ir para a etapa 7.

- No campo **Agência**, insira a agência da autoridade legal onde você relatou o furto.
- No campo **Código de país**, digite o código do país para o número de telefone.
- Nos campos **Telefone de Agência** e **Ramal**, digite o número de telefone da agência policial onde você entregou o relatório de furto.
- No campo **Distrito/Divisão/Número de Esquadra da Polícia**, digite a informação necessária.
- No campo **Número de Processo da Polícia**, digite a informação necessária.
- No campo **Responsável do Processo**, digite a informação necessária.

7. Na seção **Quem é você?**, edite as seguintes informações para a pessoa de contato autorizada na sua empresa:

- No campo **Primeiro Nome**, digite o primeiro nome do contato.
- No campo **Sobrenome**, digite o sobrenome do contato.
- No campo **Empresa**, digite o nome da sua empresa.
- No campo **Função**, digite a função deste contato.
- No campo **Endereço de E-mail**, digite o e-mail deste contato.
- No campo **Código do país**, digite o código do país para o número de telefone deste contato.
- Nos campos **Número de Telefone** e **Ramal**, digite o número de telefone para a pessoa de contato na sua empresa.

8. Na seção **Como é sua lista de contatos do relatório de furto?**, confirme a lista de contatos para este relatório de furto.

Notificações de relatórios de furto são enviados automaticamente para os indivíduos listados na lista de contatos padrão de relatórios de furto. Para ver a lista, clique em **Lista de Contatos de Relatórios de Furto**.

NOTA A Lista de Contatos de Relatórios de Furto é gerenciada somente por usuários autorizados. Para solicitar uma atualização à lista de contatos, entre em contato com um administrador com privilégios de administrador de segurança.

Se você deseja também enviar notificações para uma ou mais outras pessoas:

a) Selecione **Para este relatório de furto só, identifique qualquer pessoa que você desejar que seja atualizada para além das pessoas na Lista de Contatos de Relatórios de Furto**.

b) No campo, digite o endereço de e-mail de cada contato, separados por um ponto e vírgula.

9. Depois de concluir a inserção de informações no relatório, clique no botão **Enviar este relatório**.

   A página Criar e Editar Relatório de Furto se atualiza com as informações que você inseriu e é apresentada novamente para você verificar que o relatório está correto.

   NOTA Se você precisa fazer alterações adicionais, clique em **Editar este relatório**. A página Criar e Editar Relatórios de Furto se abre onde você faz as alterações necessárias e clica em **Enviar este Relatório**. Consulte "Editando Relatórios de Furto Existentes" na página 385.

10. Quando você estiver satisfeito de que as informações contidas no relatório sejam precisas, clique em **Este relatório está correto**.

11. Uma página de confirmação se abre com as informações sobre o relatório de furto que você acabou de criar e mostra o **número de arquivo** do relatório.

    A partir desta página de confirmação, é possível fazer o seguinte:

    - Clicar no link **número do arquivo** para abrir o relatório que você acabou de criar.
    - Clique no link **Resumo de Relatórios de Furto** para abrir essa página. Veja a grelha de resultados para uma lista dos Relatórios de Furto da sua empresa e você poderá encontrar seu novo relatório no topo da lista.
    - Clique **Criar Outro Relatório de Furto** para criar um novo Relatório de Furto.

Capítulo 16: Computrace Mobile Theft Management Mobile Theft Management para Dispositivos Chrome

O serviço de Computrace® Mobile Theft Management (CT MTM) permite que você salvaguarde seus dispositivos Chromebook e Chromebox em casos de perda ou furto. Este serviço fornece as duas seguintes componentes importantes:

- ***Prevenção de perdas para Escolas e Outras Organizações***

  É possível implementar as melhores práticas nas escolas em todo seu distrito escolar ou na sua empresa para certificar que os dispositivos são tratados com responsabilidade. Este programa foca no ensino a estudantes e usuários finais de como evitar se tornar alvos para criminosos ao usar as melhores práticas e ações seguras.

  A combinação de processos formais para o relato de dispositivos perdidos ou furtados, de etiquetas de identidade em dispositivos gerenciados, e do auxílio na percepção do usuário e na aprendizagem pode resultar em uma diminuição da quantidade total de perdas e furtos.

  Para mais informações, consulte o seguinte site:

  www.absolute.com/en/products/mobile-theft-management

- ***Investigação de Furto***

  Quando um furto é relatado, a equipe de Investigações da Absolute inicia o serviço de resposta rápida, começa uma investigação para coletar informações e evidências para as autoridades legais, e prepara relatórios investigativos e outros trabalhos críticos para o caso.

  Dependendo do contrato específico de sua empresa com a Absolute Software, o programa de Investigação de Furtos pode incluir uma garantia de serviço caso a equipe não consiga recuperar um dispositivo Chrome. Para mais informações, consulte "Compreendendo o Saldo Pré-Pago da Garantia de Serviço" na página 381.

Resumo Geral do CT MTM para Dispositivos Chrome

O agente Computrace não pode ser instalado em um dispositivo Chrome. Portanto, para gerenciar dispositivos Chrome e enviar relatórios de furto na Central do Cliente no caso de furtos, as seguintes componentes estão disponíveis para serviço do CT MTM para dispositivos Chrome:

- Uma configuração de conta da Central do Cliente para associar a sua conta do Google à sua conta da Central do Cliente.
- Um serviço de sincronização para extrair informações de dispositivos atualizadas regularmente da sua conta do Google e mostrá-las em relatórios da Central do Cliente
- Um aplicativo específico do dispositivo (aplicativo de quiosque Chrome) que você baixa da Central do Cliente e instala em um dispositivo furtado usando o Painel de Controle do desenvolvedor Google e o Google Admin Console. O aplicativo de quiosque ajuda a equipe de Investigações Absolute com a recuperação do dispositivo.

Este capítulo inclui as seguintes seções:

- Desativando Dispositivos Chrome

Gerenciando Dispositivos Chrome na Central do Cliente

Os dispositivos Chrome executam o sistema operacional Chrome OS, que é um sistema operacional leve baseado no Linux projetado para executar tanto aplicativos web como aplicativos instalados, mas a maior parte de dados de usuários é armazenada online, em vez de no disco rígido do dispositivo. Devido à natureza única deste sistema operacional, o agente Computrace não pode ser instalado em um dispositivo Chrome e chamadas de agente para o Centro de Monitoramento não são possíveis. Em vez disso, um método alternativo—o serviço de sincronização Google—é utilizado para adicionar dispositivos Chrome à Central do Cliente e manter informações de dispositivo atualizadas sobre cada dispositivo Chrome.

Esta seção oferece informações acerca dos seguintes tópicos:

- Pré-requisitos
- Sobre o Serviço de Sincronização Google
- Gerenciando Informações da Conta do Google na Central do Cliente
- Visualizando Informações de Dispositivo de um Dispositivo Chrome

Pré-requisitos

Para gerenciar dispositivos Chrome na Central do Cliente, os seguintes pré-requisitos devem ser cumpridos:

- Os dispositivos devem ser Chromebooks ou Chromeboxes executando versão 36 ou superior do sistema operacional Chrome OS.
- Os dispositivos Chrome devem estar inscritos no seu domínio usando o Google Admin console. Para mais informações sobre como inscrever dispositivos, consulte a ajuda de administrador da Google para dispositivos Chrome.
- A sua conta do Google deve ter pelo menos um administrador a quem está atribuído a função de administrador com os seguintes privilégios:
  - **Unidades organizacionais**, incluindo privilégios de **Criar**, **Ler**, **Atualizar** e **Excluir**
  - **Usuários**, incluindo privilégios de **Criar**, **Ler**, **Atualizar** e **Excluir**
  - **Serviços** > **Chrome OS**, incluindo privilégios de **Gerenciar Dispositivo**, **Gerenciar Entregas de Dispositivos**, **Gerenciar Configurações de Usuários** e **Gerenciar Configurações de Dispositivos**.

  Estes privilégios estão atribuídos à função de Super Administrador por padrão ou você pode criar uma função criada pelo usuário e atribuir estes privilégios a ela. Para mais informações sobre as funções e privilégios do Google Admin, consulte a Ajuda do Google Admin console.
- No Google Admin console, a configuração de dispositivo **Reinscrição Forçada** deve estar ativa para a sua unidade organizacional. Esta configuração certifica que se uma redefinição de fábrica for realizada em um dispositivo inscrito, um usuário não possa entrar no dispositivo Chrome sem primeiro inscrever o dispositivo em seu domínio.

Sobre o Serviço de Sincronização Google

Atualmente, usa-se o Google Admin console para gerenciar os Chromebooks e Chromeboxes inscritos na sua conta do Google. Para gerenciar estes dispositivos Chrome na Central do Cliente, você precisa adicionar o nome de sua conta do Google às suas configurações de conta da Central do Cliente. A Central do Cliente depois usa o serviço de sincronização Google para recuperar informações sobre cada dispositivo Chrome de sua conta do Google, atribui um identificador a cada dispositivo na Central do Cliente e ativa os dispositivos. Uma vez por dia, o serviço de sincronização recupera as informações mais recentes sobre cada dispositivo da sua conta do Google e atualiza as informações do dispositivo na Central do Cliente.

Limitações do Serviço de Sincronização

As informações de dispositivo Chrome disponíveis na Central do Cliente estão limitadas àquilo que está disponível no Google Admin console. Algumas informações que não estão disponíveis, tais como Nome de dispositivo, Nome de usuário e Número do ativo aparecem como “Desconhecido” na Central do Cliente. Além disso, a marca de cada dispositivo Chrome é relatada como “Chromebook” e o modelo não é fornecido.

Como o agente Computrace não pode ser instalado em um dispositivo Chrome, a seguinte funcionalidade da Central do Cliente não é suportada em dispositivos Chrome:

- Alertas
- Exclusão de Dados
- Congelamento do Dispositivo
- Mensagens do Usuário Final
- Geolocalização e Cercas Geográficas

Além disso, dispositivos Chrome estão somente incluídos nos seguintes relatórios da Central do Cliente:

- Relatório de Ativos
- Relatório do Histórico de Chamadas
- Relatório de Dispositivos Desaparecidos
- Relatório de Ativação
- Relatório de Prontidão do Dispositivo
- Relatório das Atualizações do Sistema Operacional
- Relatório de Anti-Malware em Falta
- Relatório de Dados Introduzidos pelo Usuário
- Relatório Perfis de Chamadas

Para mais informações sobre estes relatórios, consulte "Trabalhando com Relatórios" na página 152.

NOTA Em relatórios que incluem horas de chamadas, este valor é a data e a hora em que as informações do dispositivo Chrome na Central do Cliente foram sincronizadas com as informações na conta do Google do dispositivo.

Gerenciando Informações da Conta do Google na Central do Cliente

Esta seção oferece informações acerca dos seguintes tópicos:

- Adicionando Informações da Conta do Google à Central do Cliente

- Excluindo Informações de Conta do Google

Adicionando Informações da Conta do Google à Central do Cliente

Para dispositivos Chrome que são atualmente gerenciados na sua conta do Google serem visíveis na Central do Cliente, é preciso adicionar o nome de sua conta do Google à sua conta da Central do Cliente. Este processo habilita o serviço de sincronização a recuperar informações sobre cada dispositivo Chrome de sua conta do Google, atribuir um identificador a cada dispositivo na Central do Cliente e ativar os dispositivos.

Para adicionar o nome de sua conta do Google à sua conta da Central do Cliente:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Configurações de Conta**.
3. Role para a área **Chromebooks - Conta do Google** e no campo **Nome de Conta** insira o endereço de e-mail que você usa para se conectar à conta do Google da sua empresa.

   IMPORTANTE Você não poderá definir esta configuração se não for atribuído uma função do Google Admin que inclua um conjunto mínimo de privilégios de administrador. Para mais informações sobre estes privilégios necessários, consulte "Pré-requisitos" na página 362.

4. Clique em **Adicionar**.
5. Se você não estiver já conectado à sua conta do Google, a página de entrada do Google se abre. Conecte-se usando as credenciais certas.
6. A página Solicitação para Permissão da Google se abre e permite-lhe autorizar o serviço de sincronização. Este serviço sincroniza as informações de dispositivos na Central do Cliente com as informações mantidas no Google Admin console. Ele também permite que o processo de recuperação por furto seja iniciado a partir da Central do Cliente caso um dispositivo Chrome seja perdido ou furtado. Clique em **Aceitar**.

   Uma mensagem aparece na página Configurações de Conta informando que a conta do Google foi adicionada. Todos os dispositivos Chrome associados a esta conta do Google são adicionadas à conta do Google.

Excluindo Informações de Conta do Google

Se uma conta do Google foi adicionada indevidamente, ou a conta já não é mais necessária, é possível excluí-la a partir da página Configurações de Conta.

Excluindo uma conta do Google existente tem o seguinte efeito sobre dispositivos Chrome adicionados à Central do Cliente.

- Os dispositivos Chrome da conta do Google são definidos como Desativados na Central do Cliente.

  NOTA Dispositivos Chrome com um relatório de furto permanecem definidos como Furtados na Central do Cliente.

- As informações de dispositivo já não estão sincronizadas entre a conta do Google e a Central do Cliente.
- Informações de dispositivo Chrome já não são incluídas nos relatórios.

- Não é possível enviar um relatório de furto para um dispositivo Chrome.

NOTA Não é possível editar um nome de uma conta do Google. Se você digitou o nome de conta incorretamente, deve excluir o registro e depois adicioná-lo novamente usando o nome correto.

Para excluir uma conta do Google:

1. Entre na Central do Cliente como um Administrador.
2. No painel de navegação, clique em **Administração** > **Conta** > **Configurações de Conta**.
3. Role para a área **Chromebooks - conta do Google**, localize a conta do Google que você deseja excluir e clique no seu link de **Excluir** na coluna da extrema direita.
4. Na mensagem de confirmação, clique em **OK**.

Visualizando Informações de Dispositivo de um Dispositivo Chrome

Para ver informações de dispositivo para um dispositivo Chrome:

1. Conecte-se à Central do Cliente e abra um relatório. Consulte "Executando Relatórios" na página 138.

   NOTA Para a lista de relatórios que incluem informações sobre seus dispositivos Chrome gerenciados, consulte "Limitações do Serviço de Sincronização" na página 363.

2. Clique no **Identificador** do dispositivo que você deseja ver.

   A página Resumo do Dispositivo fornece as seguintes informações sobre o dispositivo Chrome:

   - **Identificador**: um número de série eletrônico único atribuído ao dispositivo na Central do Cliente
   - **Marca**: aparece como **Chromebook** para tanto Chromebooks como Chromeboxes
   - **Número de Série**: o número de série do dispositivo Chrome
   - **Departamento**: o departamento ao qual o dispositivo Chrome está atribuído na Central do Cliente
   - **Nome de Usuário Atribuído**: o nome de usuário atribuído ao dispositivo Chrome na Central do Cliente
   - **E-mail de Usúario Atribuído**: o endereço de e-mail atribuído ao dispositivo Chrome na Central do Cliente
   - **Número de Ativo Atribuído**: o número de ativo atribuído ao dispositivo Chrome na Central do Cliente
   - **Grupos de Dispositivos**: mostra os grupos de dispositivos a quais este dispositivo gerenciado pertence

     Para editar um grupo de dispositivos, clique no link do grupo de dispositivos desejado. Para mais informações, consulte "Editando um Grupo de Dispositivos" na página 82.

   NOTA É possível editar valores nos campos **Departamento**, **Nome de Usuário Atribuído**, **Endereço de e-mail de usuário atribuído**, e **Número de Ativo Atribuído**.

   Os seguintes separadores fornecem mais informações sobre o dispositivo Chrome:

- Separador do **Resumo do Hardware**:
  - **Marca Detectada**:aparece como **Chromebook** para tanto Chromebooks como Chromeboxes
  - **Número de Série Detectado**: o número de série do dispositivo Chrome, como fornecido pelo serviço de sincronização
  - **Endereço MAC do Cartão de Rede 1**: o endereço de rede do cartão de rede no dispositivo, como fornecido pelo serviço de sincronização
  - **Endereço MAC do Cartão de Rede 2**: o endereço de rede do segundo cartão de rede no dispositivo, como fornecido pelo serviço de sincronização
  - **Versão do BIOS/Firmware do sistema**: o nome e número únicos da versão de firmware instalado no dispositivo Chrome, como fornecido pelo serviço de sincronização
- Separador do **Resumo de Software**:
  - **Sistema Operacional**: mostra **Chrome** para todos os dispositivos executando o sistema operacional Chrome OS
  - **AntiMalware Detectado**: mostra **Não**, já que software antimalware não é necessário em um dispositivo Chrome
- Separador do **Rastreamento de Chamadas**:
  - **Relatório do Histórico de Chamadas**: um link a este relatório

    Para ver detalhes sobre **Informações Estendidas de Chamadas de IP**, clique no link sob a coluna **Endereço de IP Público** na grelha de resultados do relatório.
  - **Agente chamou pela primeira vez em (primeira chamada)**: a data e a hora da primeira vez em que as informações de dispositivo na Central do Cliente foram sincronizadas com as informações de dispositivo na sua conta do Google.
  - **Versão de Agente**: o número de versão (22*xx*) do serviço de sincronização usado para sincronizar as informações de dispositivo na Central do Cliente com as informações de dispositivo na conta do Google do dispositivo.

    NOTA Se um relatório de furto existir para o dispositivo e o pacote de Mobile Theft Management do Chromebook estiver implantado no dispositivo, a versão de agente aparece como 23*xx*. Para mais informações, consulte "Relatando o Furto de um Dispositivo Chrome" na página 367.
  - **Última chamada do agente em**: a data e a hora da última vez em que as informações de dispositivo na Central do Cliente foram sincronizadas com as informações de dispositivo na sua conta do Google.
  - **Última chamada do agente feita de**: o campo fica em branco a não ser que um relatório de furto exista para o dispositivo, caso em que aparece **Furtado**
  - **Últimos dados de rastreamento do ativo coletados em**: a data e a hora da última vez em que as informações de dispositivo na Central do Cliente foram sincronizadas com as informações de dispositivo na sua conta do Google.

3. Se você alterou quaisquer informações de dispositivo, clique em **Salvar Alterações**. A página Resumo de Dispositivos é atualizada e confirma que suas alterações foram salvas.

Relatando o Furto de um Dispositivo Chrome

Relatando o furto de um dispositivo Chrome envolve um pouco mais etapas que o processo para outros dispositivos porque o agente Computrace não pode ser instalado em um dispositivo Chrome. Para assistir a equipe de Investigações Absolute na recuperação de um dispositivo Chrome, um pequeno aplicativo específico do dispositivo precisa estar instalado no dispositivo. Este aplicativo é chamado um aplicativo de quiosque Chrome e é implantado no dispositivo usando a web store do Chrome.

Para relatar o furto de um dispositivo Chrome furtado, você deve completar as seguintes tarefas-chave:

1. Apresente uma queixa oficial junto da sua agência de polícia local.
2. Use a Central do Cliente para enviar um relatório de furto e baixar o pacote Chrome MTM Deployment da Central do Cliente. O pacote inclui o aplicativo de quiosque Chrome para o dispositivo. Consulte "Criando um Relatório de Furto para um Dispositivo Chrome Furtado" na página 367.
3. Carregue o pacote Chrome MTM Deployment para a Web Store do Chrome. Consulte "Carregando o Pacote Chrome MTM Deployment para a Chrome Web Store" na página 370.
4. Implante o aplicativo de quiosque Chrome no dispositivo Chrome furtado. Consulte "Implantando o aplicativo de quiosque no dispositivo Chrome" na página 372.

   Para informações sobre o comportamento de um dispositivo Chrome com um aplicativo de quiosque implantado, consulte "Qual o efeito do aplicativo de quiosque Chrome implantado sobre o dispositivo furtado?" na página 374.

IMPORTANTE *Não* desative o dispositivo Chrome furtado usando o recurso Desativar disponível no Google Admin console. Este recurso interfere com a capacidade da equipe de Investigações Absolute de recuperar o dispositivo.

Depois destas tarefas-chave serem completadas, a equipe de Investigações da Absolute trabalha em conjunto com seu serviço de aplicação de lei local para localizar o dispositivo furtado. Dependendo do resultado da investigação, um dos seguintes cenários ocorre:

- Quando o dispositivo é encontrado, a equipe de Investigações da Absolute coordena a devolução do dispositivo a você.
- Se o dispositivo furtado não for recuperado e você adquiriu uma licença Premium e está elegível para uma Garantia de Serviço, que está sujeita à elegibilidade com base nos termos do seu Contrato de Serviço do Usuário Final da Absolute. Para mais informações sobre pagamentos da Garantia de Serviço, consulte "Compreendendo o Saldo Pré-Pago da Garantia de Serviço" na página 381.

NOTA Para mais informações sobre como enviar relatórios de furto, consulte "Relatando o Furto de um Dispositivo Gerenciado" na página 377.

Criando um Relatório de Furto para um Dispositivo Chrome Furtado

Para criar um relatório de furto para um dispositivo Chrome furtado:

1. Conecte-se à Central do Cliente.

2. No painel de navegação, clique em **Relatório de Furto** > **Criar e Editar Relatório de Furto**. A página Criar e Editar Relatórios de Furto se abre.
3. Na área de **Que dispositivo?** faça uma das seguintes opções para selecionar o dispositivo desejado:
   - Ao lado do campo **Escolher Dispositivo**, clique em **Escolher** para abrir o diálogo de Escolher o Identificador. Para mais informações sobre como usar o recurso **Escolher**, consulte "Editando Informações de Ativos" na página 141.

     Depois de selecionar um dispositivo, o diálogo Escolher Identificador se fecha e a página Criar e Editar Relatórios de Furto se atualiza e preenche os campos **Marca**, **Modelo**, **Número de Série**, **Número de Ativo**, e **Sistema Operacional**.
   - Digite os valores desejados nos campos **Marca**, **Modelo**, **Número de Série**, **Número de Ativo**, e **Sistema Operacional**.
4. Na área **Como é que o dispositivo foi furtado?**, faça o seguinte:

   IMPORTANTE Os campos obrigatórios são indicados por um asterisco (*).

   - Nos campos **Data e Hora do Furto**, digite a **data** (formato dd/mm/aaaa) no primeiro campo ou abra o calendário e selecione a data desejada. No segundo campo, digite a **hora** no formato hh:mm.
   - No campo **Fuso Horário**, abra a lista e selecione o Fuso Horário desejado.
   - Nos campos de **Local do Furto**, insira o endereço completo onde o furto aconteceu.
   - No campo **Nome da Vítima**,digite o nome completo da vítima.
   - Nos campo de **Cidade do Furto**, insira a cidade ou vila onde o furto aconteceu.
   - No campo **País de Furto**, abra a lista e selecione o país onde o furto aconteceu.
   - No campo **Estado/Província do Furto**, insira o estado ou a província onde o furto aconteceu.
   - Nas opções de **O cabo de alimentação foi furtado?**, clique na resposta desejada a partir de **Sim**, **Não**, e **Desconhecida**.
   - No campo **Detalhes do Furto**, insira os detalhes acerca da última localização conhecida do dispositivo e como o mesmo foi furtado.
5. Na área de **Você já registrou uma ocorrência junto à polícia?**, insira a seguinte informação usando o relatório da polícia que você preencheu quando relatou o furto às autoridades.
   - No campo **Agência**, insira a agência da autoridade legal onde você relatou o furto.
   - No campo **Código de país**, digite o código do país para o número de telefone.
   - No campo **Telefone de Agência** e **Ramal**, digite o número de telefone da agência policial onde você relatou o furto.
   - No campo **Distrito/Divisão/Número de Esquadra da Polícia**, digite a informação necessária.
   - No campo **Número de Processo da Polícia**, digite a informação necessária.
   - No campo **Responsável do Processo**, digite a informação necessária.
6. Na área **Quem é você?**, edite as seguintes informações para a pessoa de contato autorizada na sua empresa:
   - No campo **Primeiro Nome**, digite o primeiro nome do contato.

- No campo **Sobrenome**, digite o sobrenome do contato.
- No campo **Empresa**, digite o nome da sua empresa.
- No campo **Função**, digite a função deste contato.
- No campo **Endereço de E-mail**, digite o endereço de e-mail desta pessoa de contato.
- No campo **Código do país**, digite o código do país para o número de telefone deste contato.
- Nos campos **Número de Telefone** e **Ramal**, digite o número de telefone para a pessoa de contato na sua empresa.

7. Na área **Como é sua lista de contatos do relatório de furto?**, confirme a lista de contatos para este relatório de furto.

   Notificações de relatórios de furto são enviadas automaticamente para os indivíduos listados na lista de contatos padrão de relatórios de furto. Para ver a lista, clique em **Lista de Contatos de Relatórios de Furto**.

   NOTA A Lista de Contatos de Relatórios de Furto é gerenciada somente por usuários autorizados. Para solicitar uma atualização à lista de contatos, entre em contato com um administrador com privilégios de administrador de segurança.

   Se você deseja também enviar notificações para uma ou mais outras pessoas:

   a) Selecione **Para este relatório de furto só, identifique qualquer pessoa que você desejar que seja atualizada para além das pessoas na Lista de Contatos de Relatórios de Furto**.
   b) No campo, digite o endereço de e-mail de cada contato, separados por um ponto e vírgula.

8. Depois de concluir a inserção de informações no relatório, clique no botão **Enviar este relatório**.

   A página Criar e Editar Relatório de Furto se atualiza com as informações que você inseriu e é apresentada novamente para você verificar que o relatório está correto.

   NOTA Se você precisa fazer alterações adicionais, clique em **Editar este relatório**. A página Criar e Editar Relatórios de Furto se abre onde você faz as alterações necessárias e clica em **Enviar este Relatório**.

9. Quando você estiver satisfeito de que as informações contidas no relatório sejam precisas, clique em **Este relatório está correto**.

   Uma página de confirmação se abre com as informações sobre o relatório de furto que você acabou de criar e mostra o **número de arquivo** do relatório.

10. Na mensagem de aviso na página de confirmação, procure o nome da unidade organizacional Google onde o dispositivo Chrome foi movido e registre o nome cuidadosamente. O nome inclui o número de série do dispositivo.
11. Clique no link **pacote Chrome MTM Deployment da Absolute** e salve o arquivo zip produzido no seu disco rígido local. Este pacote é composto por um arquivo zip contendo o aplicativo de quiosque Chrome e as componentes necessárias para a publicação do aplicativo de quiosque Chrome na web store do Chrome.
12. Na página de confirmação, execute quaisquer das seguintes ações:

    - Clicar no link **número do arquivo** para abrir o relatório que você acabou de criar.

- Clique no link **Resumo de Relatórios de Furto** para ver a lista de relatórios de furto de sua empresa. Seu novo relatório estará no topo da lista.
- Clique **Criar Outro Relatório de Furto** para criar um novo Relatório de Furto.

13. Vá para a tarefa, "Carregando o Pacote Chrome MTM Deployment para a Chrome Web Store" na página 370.

Baixando o pacote Chrome MTM Deployment de um Dispositivo

Se você não baixou o pacote Chrome MTM Deployment quando enviou o relatório de furto, pode baixá-lo da página Criar e Editar Relatório de Furto do dispositivo.

Para baixar o pacote Chrome MTM Deployment para um dispositivo Chrome furtado:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Relatório de Furto** > **Resumos de Relatórios de Furto**.
3. Na página Resumo de Relatório de Furto, use os campos na área Critérios de Pesquisa para procurar o dispositivo Chrome furtado.
4. Na grelha de resultados, clique no link **Ver** do dispositivo. A página Criar e Editar Relatórios de Furto se abre.
5. Clique no link ao lado de **Pacote de Download** e salve o arquivo zip no seu disco rígido local. Este pacote é composto por um arquivo zip contendo o aplicativo de quiosque e as componentes necessárias para a publicação de um aplicativo de quiosque na web store do Chrome.
6. Vá para a tarefa, "Carregando o Pacote Chrome MTM Deployment para a Chrome Web Store" na página 370.

Carregando o Pacote Chrome MTM Deployment para a Chrome Web Store

Para implantar o aplicativo de quiosque Chrome no dispositivo furtado, você necessita carregar o conteúdo do pacote Chrome MTM Deployment para a web store do Chrome e publicá-lo como um aplicativo não listado para que ele não seja visível ao público geral.

Para carregar o pacote Chrome MTM Deployment para a Web Store do Chrome:

1. No seu computador, navegue para o local onde você salvou o pacote Chrome MTM Deployment do dispositivo na etapa 11 da tarefa, "Relatando o Furto de um Dispositivo Chrome" na página 367.
2. Extraia o arquivo zip. O pacote contém um arquivo `agent.zip`, instruções para implantação e alguns arquivos de imagem.
3. Conecte-se ao Painel de Controle do desenvolvedor Chrome em https://chrome.google.com/webstore/developer/dashboard?authuser=1

   NOTA Se esta é a sua primeira vez publicando um aplicativo na Web Store do Chrome usando o Painel de controle do desenvolvedor, a Google exige que você pague uma taxa única de adesão.

4. Role para a parte baixa da página Painel de controle do desenvolvedor e clique em **Adicionar novo item**.

5. Sob Fazer upload de uma extensão ou aplicativo (arquivo .zip) clique em **Escolher arquivo**.
6. Navegue para o arquivo `agent.zip` incluído no pacote extraído e selecione-o. O nome do arquivo aparece sob **Enviar uma extensão ou aplicativo (arquivo .zip)**.
7. Clique em **Enviar**. O arquivo é carregado e a página Editar Item aparece. O pacote que você enviou aparece na área Carregamentos.
8. Na área do ícone:
   a) Clique em **Enviar novo ícone**.
   b) Na caixa de diálogo que abre, clique em **Escolher arquivo** e selecione o arquivo `icon_128x128.png`.
   c) Clique em **Enviar**. A imagem do ícone aparece na área do ícone.
9. Na área Capturas de tela:
   a) Clique em **Escolher**.
   b) Na caixa de diálogo que abre, selecione o arquivo `screenshot_1280x800.png`. A imagem de miniatura aparece na área Capturas de tela.
10. Na área das imagens de bloco promocionais:
    a) Ao lado de **Bloco pequeno** clique em **Enviar nova imagem**.
    b) Na caixa de diálogo que abre, clique em **Escolher arquivo** e selecione o arquivo `promo_440x280.png`.
    c) Clique em **Enviar**. Um link de **Ver atual** aparece adjacente a **Bloco pequeno**. Para visualizar a imagem, clique no link.
11. Clique no campo **Categoria** e sob Ferramentas de Negócio selecione **Administração e Gerenciamento**.
12. Clique no campo **Idioma** e selecione o idioma aplicável.
13. Sob as opções de Visibilidade, selecione **Não listado**, que publica o aplicativo de forma que ele não seja visível ao público geral.

    IMPORTANTE Não ignore esta etapa.

14. Clique em **Publicar alterações**.
15. Na mensagem de confirmação, clique em **OK**. Uma caixa de diálogo se abre, mostrando o nome do pacote que você carregou.
16. Na faixa na parte superior da página, clique em **Retornar para Painel de controle**. O pacote carregado aparece no topo da lista no Painel de controle do desenvolvedor.
17. Se esta for a primeira vez que você envia um relatório de furto para um dispositivo Chrome, vá para a próxima tarefa, Definindo as Configurações Padrão para Dispositivos Chrome Furtados. Se você já definiu a configuração padrão para unidade organizacional furtada, vá para a tarefa, "Implantando o aplicativo de quiosque no dispositivo Chrome" na página 372.

Definindo as Configurações Padrão para Dispositivos Chrome Furtados

Na sua conta do Google, uma unidade organizacional “furtada” é criada automaticamente a primeiro vez que um dispositivo Chrome é relatado como furtado na Central do Cliente. Para facilitar o processo de relato de furtos, é prática recomendada definir configurações de dispositivo padrão para a unidade organizacional furtada. Esta configuração assegura que todos os dispositivos furtados herdem as mesmas configurações.

NOTA Você precisa completar esta tarefa apenas uma vez.

Para definir configurações de dispositivo padrão para a unidade organizacional furtada:

1. Conecte-se ao Google Admin console em admin.google.com usando a conta do Google de seu domínio.

   IMPORTANTE Para completar esta tarefa, você deve se conectar como um administrador com privilégio **Serviços** > **Chrome OS**. Este privilégio está atribuído à função de Super Administrador por padrão ou você pode criar uma função criada pelo usuário e atribuir este privilégio a ela. Para mais informações sobre as funções e privilégios do Google Admin, consulte a Ajuda do Google Admin console.

2. Clique em **Gerenciamento de dispositivo**.
3. Na página Gerenciamento de dispositivo, clique em **Gerenciamento Chrome**.
4. Clique em **Configurações do dispositivo**.
5. Sob Organizações, clique na organização **Furtado** para a abrir.
6. Na página de Configurações da organização, clique no campo **Reinscrição**, e da lista que aparece, selecione **Forçar dispositivo a reinscrever-se neste domínio depois do apagamento**.
7. Clique no campo **Modo de Convidado** e selecione **Não permitir modo de convidado** da lista.
8. Clique no campo **Restrição de Entrada** e selecione **Não permitir entrada a qualquer usuário** da lista.
9. Role para a seção de Configurações de Quiosque, clique no campo **Quiosque de Sessão Pública** e selecione **Não permitir Quiosque de Sessão Pública**. Deixe o campo **Quiosque de aplicativo único** definido como **Não permitir quiosque de aplicativo único**.
10. Role para a seção Relato de Dispositivos e faça o seguinte:
    a) Clique no campo **Relato do Estado de Dispositivos** e selecione **Ativar o relato do estado de dispositivos** da lista.
    b) Clique no campo **Rastreamento do Usuário de Dispositivos** e selecione **Ativar o rastreamento de usuários recentes de dispositivos** da lista.
11. Clique em **Salvar Alterações**.

Implantando o aplicativo de quiosque no dispositivo Chrome

O aplicativo de quiosque Chrome é único em cada dispositivo. Para implantar o aplicativo de quiosque apropriado no dispositivo Chrome furtado, você precisa associar o aplicativo à unidade organizacional do dispositivo.

NOTA Quando você envia o relatório de furto para um dispositivo furtado, uma unidade organizacional é criada dentro da unidade organizacional furtada e o dispositivo furtado é transferido para dentro dela. O número de série do dispositivo está incluído no nome da unidade organizacional. Todas as configurações aplicadas à unidade organizacional furtada são herdadas pela unidade organizacional do dispositivo furtado.

Para implantar o aplicativo de quiosque Chrome no dispositivo Chrome furtado:

1. Conecte-se ao Google Admin console em admin.google.com usando a conta do Google de seu domínio.

   IMPORTANTE Para completar esta tarefa, você deve se conectar como um administrador com privilégio **Serviços** > **Chrome OS**. Este privilégio está atribuído à função de Super Administrador por padrão ou você pode criar uma função criada pelo usuário e atribuir este privilégio a ela. Para mais informações sobre as funções e privilégios do Google Admin, consulte a Ajuda do Google Admin console.

2. Clique em **Gerenciamento de dispositivo**.
3. Na página Gerenciamento de dispositivo, clique em **Gerenciamento Chrome**.
4. Clique em **Configurações do dispositivo**.
5. Sob Organizações, localize o nome da unidade organizacional que inclui o número de série do dispositivo e clique no link. A página de Configurações do dispositivo se abre.
6. Role para a seção de Configurações de Quiosque, clique no campo **Quiosque de Aplicativo Único** e selecione **Permitir Quiosque de Aplicativo Único**.
7. Clique no link de **Gerenciar aplicativos de quiosque**.
8. No diálogo do aplicativo de quiosque:
   a) Clique em **Aplicativos do Domínio**.
   b) Na lista de aplicativos que se abre, procure o pacote que você carregou na tarefa, "Carregando o Pacote Chrome MTM Deployment para a Chrome Web Store" na página 370. O nome do pacote inclui o número de série do dispositivo.

      NOTA Pode demorar até 60 minutos para o aplicativo de quiosque Chrome aparecer na lista de aplicativos.

   c) Clique no link de **Detalhes** do pacote para verificar se é o pacote certo. Os detalhes do pacote aparecem em uma caixa de diálogo em um novo separador do navegador. Feche o separador.
   d) Clique no link de **Adicionar** do pacote. O pacote é adicionado à lista de aplicativos sob Total para ser instalado.
   e) Clique em **Salvar**.
9. Na página Configurações do Dispositivo, na seção Configurações de quiosque, clique no campo **Inicializar Automaticamente o Aplicativo de Quiosque** e selecione da lista o pacote que adicionou na etapa 8.
10. Clique em **Salvar Alterações**.

Dependendo do período de tempo da sondagem definido para a sua conta do Google, pode demorar até 24 horas para o aplicativo de quiosque ser implantada no dispositivo furtado. Se o dispositivo for reiniciado, o aplicativo é implantado imediatamente.

Qual o efeito do aplicativo de quiosque Chrome implantado sobre o dispositivo furtado?

Após o aplicativo de quiosque Chrome ser implantado em um dispositivo Chrome furtado, as informações do dispositivo são enviadas para o Centro de Monitoramento da Absolute, onde estão disponibilizadas à equipe de Investigações Absolute para ajudar na recuperação do dispositivo.

De uma perspetiva de usuário, dispositivos furtados com um aplicativo de quiosque implantado possuem as seguintes características:

- Se um usuário iniciar o dispositivo, um navegador web se abre. O navegador web não pode ser fechado ou minimizado mas a funcionalidade total do navegador está disponível. Assim que o usuário navegar pela internet, informações de endereço IP e geolocalização são coletadas e enviadas para o Centro de Monitoramento.
- O usuário não consegue entrar na sua conta do Google, definir configurações, acessar quaisquer aplicativos Google ou adicionar um novo usuário.

Se um usuário realizar uma redefinição de fábrica no dispositivo furtado, a página **Chrome > inscrição empresarial** se abre quando o dispositivo for reiniciado. O usuário deve conectar-se ao seu domínio para proceder. Dois cenários são possíveis:

- Se o usuário inserir as credenciais certas para se conectar ao seu domínio, o dispositivo é reinscrito no seu domínio e o aplicativo de quiosque é prontamente implantado.
- Se o usuário não tiver as credenciais certas para se conectar ao seu domínio, o aplicativo de quiosque não pode ser implantado e outros métodos deverão ser utilizados para recuperar o dispositivo.

IMPORTANTE *Não* desative o dispositivo Chrome furtado usando o recurso Desativar disponível no Google Admin console. Este recurso interfere com a capacidade da equipe de Investigações Absolute de recuperar o dispositivo.

Após o dispositivo ser recuperado e a equipe de Investigações Absolute encerrar o relatório de furto, os seguintes eventos ocorrem:

- O dispositivo é transferido de volta para a sua unidade organizacional original na sua conta do Google.
- O aplicativo de quiosque é removido do dispositivo e funcionalidade total do dispositivo Chrome é restaurada.

Desativando Dispositivos Chrome

Se você verificar que um ou mais dispositivos Chrome já não estão funcionais, ou precisam ser reformados, pode desativar os dispositivos na Central do Cliente usando o recurso de remoção de agentes.

A desativação de um dispositivo Chrome altera o seu status de Ativo para Desativo e pára o serviço de sincronização que sincroniza as informações do dispositivo na Central do Cliente com as informações na sua conta do Google.

NOTA Não é possível desativar um dispositivo Chrome furtado com um Relatório de Furto aberto.

Para desativar dispositivos Chrome:

1. Conecte-se à Central do Cliente como um usuário a quem foi concedido autorização para criar solicitações de remoção de agentes. Para mais informações, consulte os seguintes tópicos:
   - "Gerenciando solicitações de remoção de agentes" na página 132
   - "Criar Novos Usuários" na página 108
2. Se sua empresa usa códigos de autorização enviados por e-mail para serviços de segurança, solicite um código de autorização ao completar a tarefa, "Solicitando um Código de Autorização de Segurança" na página 265.
3. No painel de navegação, clique em **Administração** > **Conta** > **Criar e Visualizar Solicitações de Remoção de Agentes**.
4. Na página Criar e Visualizar Solicitações de Remoção de Agentes, clique em **Criar nova solicitação para Remoção de Agentes**.
5. No diálogo de Selecionar Dispositivo(s) para Remoção de Agentes, faça o seguinte:
   a) No campo **Onde o grupo é**, abra a lista e selecione um grupo de dispositivos.
   b) Para localizar dispositivos Chrome que você deseja desativar, insira informações nos campos adjacentes a **e o campo**. Por exemplo, é possível localizar todos os dispositivos com um número de série que começa com as mesmas três letras.
   c) Por padrão, a lista de dispositivos exibida na grelha de resultados está limitada a apenas aqueles dispositivos que são elegíveis para serem desativados. Se você deseja exibir todos os dispositivos que correspondem aos critérios que você especificou, limpe a caixa de seleção **Mostrar apenas dispositivos elegíveis**.
   d) Clique em **Filtrar**. A caixa de diálogo Selecionar Dispositivo(s) para Remoção de Agentes é atualizada e mostra uma lista de dispositivos que satisfazem os seus critérios.
   e) Na grelha de resultados, selecione os dispositivos ao fazer uma das seguintes ações na coluna da extrema esquerda, que exibe caixas de seleção:
      - Para selecionar dispositivos individuais, marque as caixas de seleção para aqueles dispositivos só.
      - Para selecionar todos os dispositivos mostrados apenas nesta página, marque a caixa de seleção no cabeçalho.
      - Para selecionar todos os dispositivos que atenderam aos critérios de filtragem, focalize seu mouse sobre a seta na caixa de seleção do cabeçalho. Clique no link **Selecionar todos os registros (<n>)** para selecioná-los todos. O diálogo se atualiza e mostra todos os dispositivos selecionados.
6. Clique em **Continuar** para abrir o diálogo de Definir Dispositivo(s) para Remoção de Agentes.
7. Se você é um administrador de segurança, você será solicitado a fornecer autorização. Dependendo de que método de autenticação de segurança sua empresa escolheu, faça uma das seguintes ações:
   - Para empresas que usam Tokens RSA SecurID para serviços de segurança:
     i) Digite sua **Senha da Central do Cliente**.
     ii) Digite o **Código do Token SecurID** que aparece em seu Token RSA SecurID.

Para mais informações, consulte "Usando Tokens RSA SecurID para Serviços de Segurança" na página 263.

- Para empresas que usam códigos de autorização enviados por e-mail para serviços de segurança:
  i) Digite sua **Senha da Central do Cliente**.
  ii) Digite o **Código de Autorização** de Segurança que você recebeu na mensagem de e-mail.

  Para mais informações, consulte "Usando Códigos de Autorização Enviados por E-mail para Serviços de Segurança" na página 264.

8. Clique em **Definido para remoção**. O status do dispositivo Chrome é definido como Desativado e o serviço de sincronização é parado.

Capítulo 17: Relatando o Furto de um Dispositivo Gerenciado

Ao verificar que um de seus dispositivos foi furtado, após ter apresentado uma queixa junto das autoridades locais, você pode usar a Central do Cliente para relatar a perda ou o furto à equipe de Investigações da Absolute Software.

IMPORTANTE Os serviços de recuperação por furto estão incluídos somente nos serviços do Computrace®Plus, Computrace®Complete e Computrace®One.

Os serviços de recuperação por furto **não** são suportados em dispositivos Blackberry ou Windows Mobile.

Este capítulo inclui as seguintes informações e tarefas:

- Lista de Verificação de Envio da Garantia de Serviço e de Furto
- Visualizando Relatórios de Furto existentes e seus Históricos de Relatórios
- Criando um Relatório de Furto
- Editando Relatórios de Furto Existentes
- Clonando um Relatório Existente
- Fechando um Relatório de Furto Aberto
- Gerenciando a Lista de Contatos do Relatório de Furto

Lista de Verificação de Envio da Garantia de Serviço e de Furto

A seguinte lista de verificação fornece diretrizes para as melhores práticas para o relato de perdas ou furtos de um dispositivo e para completar o relatório de furto.

Estágio	Ação Necessária	Descrição	Ação Concluída
Tratamento do Dispositivo	Manuseie o dispositivo de um modo razoavelmente seguro.	Certifique-se de que o dispositivo não é deixado sem vigilância ou em um lugar inseguro.	

Estágio	Ação Necessária	Descrição	Ação Concluída
Relatório de Furto Se você está relatando o furto de um dispositivo iPad ou iPad mini, consulte "Computrace Mobile Theft Management para dispositivos iPad" na página 345.	De acordo com nosso Contrato de Serviço, a data do furto é a data que você descobriu o furto. Relate o furto de um dispositivo ao serviço de aplicação da lei apropriado e depois envie um relatório de furto à Absolute Software. Consulte "Criando um Relatório de Furto" na página 381.	Entre em contato com o serviço de aplicação da lei apropriado e com a Absolute Software dentro de 14 dias da detecção do furto. Nesta altura, um caso de furto é aberto na Absolute Software. Consulte "Contatando o Suporte Global da Absolute Software" na página 23. Caso você não informe a Absolute Software do furto em um prazo de 14 dias, você não estará elegível para a Garantia de Serviço. Quando o Suporte Global da Absolute receber seu Relatório de Furto, será enviado para você um e-mail confirmando a recepção de um contato da Garantia de Serviço no dia seguinte.	
Submissões da Garantia de Serviço	Você terá um prazo de 30 dias a partir do recebimento para enviar o formulário de envio preenchido da Garantia de Serviços.	Trinta dias a partir da data em que seu caso de furto foi aberto na Absolute Software, um formulário de envio da Garantia de Serviço é enviado para você para preenchimento e devolução.	
	Assegure-se de que inclua todos os recibos tanto para a aquisição original do dispositivo como para qualquer licenças profissionais que estejam associadas com o dispositivo.	O administrador da Garantia de Serviço da Absolute Software fornece reembolso pela perda do dispositivo, baseado nos recibos de compra fornecidos.	
	Apêndice B do Contrato de Serviços estipula os valores padrão que a Absolute Software aplica nas submissões da Garantia de Serviço.	Se você não devolver o formulário de envio da Garantia de Serviço preenchido dentro do prazo de 30 dias, a Absolute Software aplicará o valor padrão do dispositivo de acordo com o Contrato de Serviço e reembolsar em conformidade. Para detalhe sobre estes valores, visite nosso Acordo de Serviço em www.absolute.com/company/legal/agreements/computrace-agreement.	

Visualizando Relatórios de Furto existentes e seus Históricos de Relatórios

Para ver relatórios de furto existentes e seus históricos de relatórios:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Relatório de Furto** > **Resumos de Relatórios de Furto**.

   NOTA Se nenhum furto estiver registrado, a página Resumos de Relatórios de Furto mostra uma mensagem de **Nenhum registro encontrado**.

3. Na página Resumos de Relatórios de Furto, no local de Critérios de Pesquisa, você pode filtrar quais os relatórios de furto são mostrados na grelha de resultados, da seguinte forma:
   - Para visualizar o Histórico de Relatórios para vários Relatórios de Furto:
     i) No campo **No grupo**, abra a lista e selecione o Grupo de Dispositivos que contém o relatório de furto que você deseja ver.
     ii) No campo **e o Relatório contém a palavra-chave**, digite a palavra-chave correta.
     iii) No campo **e a data do Furto é entre**, selecione uma das seguintes opções:
        - Clique na opção **a qualquer data** para mostrar Relatórios de Furto para qualquer data.
        - Clique na opção de **nos últimos x dias** e digite o número certo de dias desde a criação do Relatório de Furto. A grelha de resultados exibe os resultados para este intervalo de tempo.
        - Clique na opção de **entre** e clique no primeiro campo para introduzir a data de início (dd/mm/aaaa) ou clique no calendário e clique na data de início desejada.
        - Faça o mesmo para o segundo campo, que é a data de fim; por exemplo, entre **12/06/2012** e **18/06/2012**.

     iv) Na área **e o status do Arquivo do Relatório de Furto é**, selecione cada status que você deseja incluir no relatório:

        NOTA Definições de status são fornecidas em: www.absolute.com/en/support/theft_report_definitions.aspx

        - Para incluir o Relatórios de Furto Ativos, marque a caixa de seleção **Ativo** e marque cada caixa de seleção que se aplica à lista que você deseja mostrar, da seguinte forma:
          – **Sob Investigação: Pesquisando**
          – **Sob Análise: Primeiro Contato Recebido**
          – **Aguardando Cliente: Dispositivo Conectando Internamente**
          – **Aguardando Cliente: Requerer Informação**
        - Para incluir o Monitoramento de Relatórios de Furto, selecione a caixa de seleção de **Monitorar**, e selecione cada caixa de seleção que se aplica à lista que você deseja mostrar, da seguinte forma:
          – **Aguardando Movimento do Dispositivo**
          – **Aguardando Primeiro Contato Posterior ao Furto**

- **Aguardando Contato Adicional do Dispositivo**
- **Política Incapaz de Prosseguir**
- **Aguardando Novas Pistas**

○ Para incluir os Relatórios de Furto Fechados, marque a caixa de seleção **Fechado** e marque cada caixa de seleção que se aplica à lista que você deseja mostrar, da seguinte forma:

- **Recuperado**
- **Polícia Recuperou**
- **Encerramento solicitado pelo cliente**
- **Exclusão Perpétua Iniciada pelo Cliente**
- **Software não instalado**
- **Recuperado-Não Furtado**
- **Cancelado**
- **Relatório de Furto Incompleto**
- **Nenhum Contato Posterior ao Furto**
- **Outro**

v) Na área de **e o status da Garantia de Pagamento é**, marque cada uma das caixas de seleção, conforme apropriado:

○ **Pago**
○ **Elegível**
○ **Negado**
○ **N/A** (não aplicável)

- Para ver o Histórico de Relatório de um único Relatório de Furto, no campo **ou a ID do Relatório é**, abra a lista e selecione o identificador de Relatórios de Furto desejado.

4. Clique em **Mostrar Resultados** para preencher a grelha de resultados com as opções que você escolheu no local dos Critérios de Pesquisa.

   Para cada Relatório de Furto apresentado, que está associado à sua conta, você poderá ver as seguintes informações:

   - **ID de Relatório** é um número de identificação único criado pela Central do Cliente.
   - **Identificador**
   - **Data do Furto**
   - **Data do Relatório**
   - **Data de Recuperação**
   - **Localização**
   - **Cidade, Estado e País**
   - **Marca, Modelo e Número de Série**
   - **Status do Dispositivo**: o status do Relatório de Furto de dispositivo.
   - **Status da Garantia**
   - **Ação**: **Ver** ou **Clonar** este relatório de furto.

5. Na grelha de resultados sob a coluna **ID de Relatório**, clique um link para abrir a página Criar e Editar Relatório de Furto onde você pode ver o histórico desse relatório.

Ver a Tabela do Histórico de Relatórios

Na parte inferior da página Resumos de Relatórios de Furto, você verá uma grelha de resultados que inclui a **ID do Relatório**, o **Identificador**, a **Data do Relatório**, a **Data de Atualização**, a **Marca**, o **Modelo**, e o número de **Série** do dispositivo desaparecido ou furtado.

Quando você clica em um link na coluna **ID de Relatório**, a página Criar e Editar Relatórios de Furto se abre para aquele relatório. A partir desta página é possível editar a informação do relatório.

A tabela do **Histórico de Relatórios** mostra um registro de todas as edições feitas ao número de um Relatório, anexado com um hífen e um número cada vez que uma edição é feita ao relatório, exemplo 84544 **-1**. Esta tabela controla o número de vezes que você edita um Resumo de Relatórios de Furto e fornece os detalhes de cada alteração registada. Sob a tabela do Histórico de Relatórios, encontrará várias opções, como se segue:

- Clique no link **Criar Outro Relatório** para criar um novo Relatório de Furto.
- Clique no link **relatórios feitos** para ver a lista de relatórios de furto de sua empresa.

Criando um Relatório de Furto

Quando um dispositivo é furtado, nós recomendamos que você apresente um Relatório de Furto às autoridades apropriadas. Para recuperar o dispositivo relatado, a equipe de Investigações da Absolute usa os detalhes fornecidos no relatório policial, que você preencheu no relatório de furto, e a informação que é coletada pelo agente no dispositivo furtado.

Caso o dispositivo furtado esteja elegível para um pagamento da Garantia do Serviço, a Absolute Software entrará em contato com você quando você se tornar elegível para receber o pagamento.

Em alguns casos, sua conta poderá conter um Saldo Pré-pago da Garantia de Serviço, que será explicado a seguir: Este saldo pré-pago influencia a sua elegibilidade para a quantidade paga da Garantia de Serviço.

Esta seção inclui a seguinte informação:

- Compreendendo o Saldo Pré-Pago da Garantia de Serviço
- Antes de começar
- Relatando um Dispositivo Furtado

Compreendendo o Saldo Pré-Pago da Garantia de Serviço

Se um dos seus dispositivos de um relatório de furto anterior for recuperado dentro de 30 dias após você receber o pagamento da Garantia de Serviço, essa quantidade paga da Garantia de Serviço que você recebeu será considerada um saldo Pré-Pago da Garantia de Serviço para a sua conta.

Em tais casos, em vez de você devolver a quantidade para a Absolute Software, o saldo Pré-Pago da Garantia de Serviço se aplicará em qualquer pagamento futuro da Garantia de Serviço que você possa receber.

Por exemplo, se você recebeu US$500 por conta de um pagamento da Garantia de Serviço pelo dispositivo 1. E vamos supor que o dispositivo 1 é recuperado 10 dias após você receber o pagamento. Passado algum tempo, você perde outro dispositivo, o dispositivo 2, com o valor de US$900 e que está elegível para um pagamento da Garantia de Serviço. Quando você receber o pagamento para o dispositivo 2, você receberá US$400, visto que sua conta contém um saldo Pré-Pago da Garantia de Serviço de US$500 e já recebeu US$500 do valor de US$900 do dispositivo 2.

Para mais informações, clique no link do **Contrato de Serviço** em qualquer página da Central do Cliente, para ver o documento da Garantia de Serviço que se aplica à sua conta.

Consultando o Saldo Pré-Pago da Garantia de Serviço

Seu Saldo Pré-Pago da Garantia de Serviço é lhe mostrado quando você preencher e entregar um novo Relatório de Furto.

Se você quiser saber seu saldo pré-pago da Garantia de Serviço sem preencher e entregar um novo Relatório de Furto, por favor contate o Suporte Global da Absolute Software. Para informações sobre como entrar em contato com o Suporte Global da Absolute Software, consulte "Contatando o Suporte Global da Absolute Software" na página 23.

Antes de começar

Antes de poder relatar um dispositivo como furtado, você precisa de atender aos seguintes pré-requisitos:

- O dispositivo não foi congelado por uma solicitação de Congelamento de Dispositivo nem por uma política de Congelamento de Dispositivo do Estado Offline. Se o dispositivo furtado estiver congelado, você deve descongelar o dispositivo antes de continuar. Para mais informações, consulte "Descongelando um Dispositivo Congelado" na página 327.
- O dispositivo não foi atribuído a nenhuma política de Congelamento de Dispositivo do Estado Offline. Você deve remover o dispositivo da política do Estado Offline antes de continuar. Para mais informações, consulte "Removendo Dispositivos de uma Política do Estado Offline" na página 320.
- Se você gostaria de executar uma solicitação de Exclusão de Dados no dispositivo, crie e lance uma solicitação de Exclusão de Dados no dispositivo **antes** de apresentar um Relatório de Furto. Para informações sobre como executar uma solicitação de Exclusão de Dados, consulte "Solicitando uma operação de Exclusão de Dados" na página 271.

Relatando um Dispositivo Furtado

NOTA Se você está relatando a perda ou furto de um dispositivo de iPad ou iPad mini, consulte "Relatando um Furto Usando a Central do Cliente" na página 358. Se você está relatando a perda ou furto de um dispositivo Chrome, consulte "Relatando o Furto de um Dispositivo Chrome" na página 367.

Para criar um relatório de furto para um dispositivo equipado com um agente que foi furtado:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Relatório de Furto**.
3. Na página Relatórios de Furto ou no painel de navegação, faça uma das seguintes ações para abrir a página Criar e Editar Relatórios de Furto:
   - Clique no link **Criar e Editar Relatórios de Furto**.
   - Clique em **Resumo de Relatórios de Furto** e na página de Resumos de Relatórios de Furto, clique em **Criar Relatório de Furto**. A página Criar e Editar Relatórios de Furto se abre.
4. Na área de **Que dispositivo?** faça uma das seguintes opções para selecionar o dispositivo desejado:

- Clique em **Escolher** para abrir o diálogo de Escolher o Identificador, onde se clica no registro desejado de uma lista de todos os dispositivos detectados para selecioná-lo. Para mais informações sobre o recurso **Escolher**, .consulte "Editando Informações de Ativos" na página 141.

  O diálogo Escolher Identificador se fecha e a página Criar e Editar Relatórios de Furto se atualiza e preenche os campos **Marca**, **Modelo**, **Número de Série**, **Número de Ativo**, e **Sistema Operacional**.
- Digite os valores desejados nos campos **Marca**, **Modelo**, **Número de Série**, **Número de Ativo**, e **Sistema Operacional**.

5. Na área **Como é que o dispositivo foi furtado?**, faça o seguinte:

NOTA Quanto mais precisas e detalhadas forem as informações fornecidas, maior a probabilidade de que a polícia possa ajudar a facilitar a recuperação. Os campos obrigatórios são indicados por um asterisco (*).

- Nos campos **Data e Hora do Furto**, digite a **data** (formato dd/mm/aaaa) no primeiro campo ou abra o calendário e selecione a data desejada. No segundo campo, digite a **hora** no formato hh:mm.
- No campo **Fuso Horário**, abra a lista e selecione o Fuso Horário desejado.
- Nos campos de **Local do Furto**, insira o endereço completo onde o furto aconteceu.
- No campo **Nome da Vítima**,digite o nome completo da vítima.
- Nos campo de **Cidade do Furto**, insira a cidade ou vila onde o furto aconteceu.
- No campo **País de Furto**, abra a lista e selecione o país onde o furto aconteceu.
- No campo **Estado/Província do Furto**, insira o estado ou a província onde o furto aconteceu.
- Nas opções de **O cabo de alimentação foi furtado?**, clique na resposta desejada a partir de **Sim**, **Não**, e **Desconhecida**.
- No campo **Detalhes do Furto**, insira os detalhes acerca da última localização conhecida do dispositivo e como o mesmo foi furtado.

6. Na área de **Você já registrou uma ocorrência junto à polícia?**, insira a seguinte informação usando o relatório da polícia que você preencheu quando relatou o furto às autoridades.

- No campo **Agência**, insira a agência da autoridade legal onde você relatou o furto.
- No campo **Código de país**, digite o código do país para o número de telefone.
- No campo **Telefone de Agência** e **Ramal**, digite o número de telefone da agência policial onde você relatou o furto.
- No campo **Distrito/Divisão/Número de Esquadra da Polícia**, digite a informação necessária.
- No campo **Número de Processo da Polícia**, digite a informação necessária.
- No campo **Responsável do Processo**, digite a informação necessária.

7. Na seção de **Quem é você?**, edite as seguintes informações para o contato autorizado da sua empresa:

- No campo **Primeiro Nome**, digite o primeiro nome do contato.
- No campo **Sobrenome**, digite o sobrenome do contato.
- No campo **Empresa**, digite o nome da sua empresa.

- No campo **Função**, digite a função deste contato.
- No campo **Endereço de E-mail**, digite o endereço de e-mail desta pessoa de contato.
- No campo **Código do país**, digite o código do país para o número de telefone deste contato.
- No campo **Número de Telefone** e **Ramal**, digite o número de telefone para a pessoa de contato na sua empresa.

8. Na seção **Como é sua lista de contatos do relatório de furto?**, confirme a lista de contatos para este relatório de furto.

   Notificações de relatórios de furto são enviadas automaticamente para os indivíduos listados na lista de contatos padrão de relatórios de furto. Para ver a lista, clique em **Lista de Contatos de Relatórios de Furto**.

   NOTA A Lista de Contatos de Relatórios de Furto é gerenciada somente por usuários autorizados. Para solicitar uma atualização à lista de contatos, entre em contato com um administrador com privilégios de administrador de segurança.

   Se você deseja também enviar notificações para uma ou mais outras pessoas:

   a) Selecione **Para este relatório de furto só, identifique qualquer pessoa que você desejar que seja atualizada para além das pessoas na Lista de Contatos de Relatórios de Furto**.
   b) No campo, digite o endereço de e-mail de cada contato, separados por um ponto e vírgula.

9. Depois de concluir a inserção de informações no relatório, clique no botão **Enviar este relatório**.

   A página Criar e Editar Relatório de Furto se atualiza com as informações que você inseriu e é apresentada novamente para você verificar que o relatório está correto.

   NOTA Se você precisa fazer alterações adicionais, clique em **Editar este relatório**. A página Criar e Editar Relatórios de Furto se abre onde você deve efetuar as alterações necessárias e clicar em **Enviar este Relatório**.

10. Quando você estiver satisfeito de que as informações contidas no relatório sejam precisas, clique em **Este relatório está correto**.
11. Uma página de confirmação se abre com as informações sobre o relatório de furto que você acabou de criar e mostra o **número de arquivo** do relatório.

    A partir desta página de confirmação, é possível fazer o seguinte:

    - Clicar no link **número do arquivo** para abrir o relatório que você acabou de criar.
    - Clique no link **Resumo de Relatórios de Furto** para abrir essa página. Veja a grelha de resultados para uma lista dos Relatórios de Furto da sua empresa e você poderá encontrar seu novo relatório no topo da lista.
    - Clique **Criar Outro Relatório de Furto** para criar um novo Relatório de Furto.

Na Central do Cliente, o dispositivo é sinalizado como furtado. Enquanto a equipe de Investigações Absolute investiga o furto, é possível ver o dispositivo na página Resumo de Relatório de Furto e no Relatório de Ativos. Para mais informações, consulte os seguintes tópicos:

- "Visualizando Relatórios de Furto existentes e seus Históricos de Relatórios" na página 379
- "Relatório de Ativos" na página 153

Editando Relatórios de Furto Existentes

Para editar as informações de um relatório de furto existente:

1. Conecte-se à Central do Cliente.
2. No painel de navegação, clique **Relatório de Furto** > **Resumos de Relatórios de Furto**.
3. Na página de Resumos de Relatórios de Furto na grelha de resultados, clique no link **ID de Relatório** para o relatório desejado.

   Uma versão de somente leitura da página **Criar e Editar Relatório de Furto** para o relatório selecionado se abre.
4. Para editar o relatório, clique em **Atualizar**.

   A página **Criar e Editar Relatório de Furto** para o relatório selecionado se abre. Na área de **Que dispositivo?**, os campos são preenchidos com informações que você não pode alterar.
5. Edite as informações que você deseja alterar, da seguinte forma:

   a) Na seção de **Como é que o dispositivo foi furtado?** edite as seguintes informações:
      - No campo **Data e Hora do Furto**, insira a nova **data** (no formato dd/mm/aaaa) ou abra o calendário e selecione a data desejada. No campo **hora**, digite a hora no formato hh:mm.
      - No campo **Fuso Horário**, abra a lista e selecione o Fuso Horário desejado.
      - No campo **Local do Furto**, digite o endereço nas linhas fornecidas.
      - No campo **Nome da Vítima**, digite o nome da vítima.
      - No campo **Cidade do Furto**, digite a cidade ou vila mais próxima de onde o furto aconteceu.
      - No campo **País de Furto**, abra a lista e selecione o país onde o furto aconteceu.
      - No campo **Estado/Província do Furto**, insira o estado ou a província onde o furto aconteceu.
      - Nas opções de **O cabo de alimentação foi furtado?** clique em uma das seguintes opções:
        - **Sim**
        - **Não**
        - **Desconhecido**
      - No campo **Detalhes do Furto**, digite os detalhes acerca da última localização conhecida do dispositivo e como o mesmo foi furtado.

   b) Na seção de**Você já registrou uma ocorrência junto à polícia?**, edite as seguintes informações do relatório policial que você entregou:
      - No campo **Agência**, digite a agência policial onde você relatou o furto.
      - No campo **Código de país**, digite o código do país para o número de telefone.
      - No campo **Telefone de Agência**, digite o número de telefone da agência policial onde você relatou o furto.
      - No campo **Ext**, digite a extensão telefônica se for aplicável.
      - No campo **Distrito/Divisão/Número de Esquadra da Polícia**, digite a informação necessária.
      - No campo **Número de Processo da Polícia**, digite a informação necessária.
      - No campo **Responsável do Processo**, digite a informação necessária.

c) Na seção de **Quem é você?**, edite as seguintes informações para o contato autorizado da sua empresa:
   - No campo **Primeiro Nome**, digite o primeiro nome do contato.
   - No campo **Sobrenome**, digite o sobrenome do contato.
   - No campo **Empresa**, digite o nome da sua empresa.
   - No campo **Função**, digite a função deste contato.
   - No campo **Endereço de E-mail**, digite o e-mail deste contato.
   - No campo **Código do país**, digite o código do país para o número de telefone deste contato.
   - No campo **Número de Telefone**, digite o número de telefone para o contato em sua empresa.
   - No campo **Ext**, digite a extensão telefônica se for aplicável.

d) Na seção **Como é sua lista de contatos do relatório de furto?**, confirme a lista de contatos para este relatório de furto.

   Notificações de relatórios de furto são enviados automaticamente para os indivíduos listados na lista de contatos padrão de relatórios de furto. Para ver a lista, clique em **Lista de Contatos de Relatórios de Furto**.

   NOTA A Lista de Contatos de Relatórios de Furto é gerenciada somente por usuários autorizados. Para solicitar uma atualização à lista de contatos, entre em contato com um administrador com privilégios de administrador de segurança.

   Se você deseja também enviar notificações para uma ou mais outras pessoas:

   i) Selecione **Para este relatório de furto só, identifique qualquer pessoa que você desejar que seja atualizada para além das pessoas na Lista de Contatos de Relatórios de Furto**.

   ii) No campo, digite o endereço de e-mail de cada contato, separados por um ponto e vírgula.

6. Quando você se sentir satisfeito de que tenha feito todas as alterações necessárias, clique em**Salvar**.

   Uma página de confirmação é aberta, indicando que o relatório foi atualizado e uma cópia do relatório atualizado será enviada para você por e-mail.

Clonando um Relatório Existente

Quando vários dispositivos são furtados ao mesmo tempo e a partir do mesmo local, você pode criar um único relatório de furto com todos os detalhes e depois clonar esse relatório de furto para cada outro dispositivo que foi perdido ou furtado.

Quando você especifica cada dispositivo perdido ou furtado que você deseja que use o relatório de furto clonado, a Central do Cliente atribui automaticamente uma nova **ID de Relatório** a cada dispositivo.

Para clonar um relatório existente:

1. Crie um Relatório de Furto para um dos dispositivos perdidos ou furtados ao completar a tarefa, "Relatando um Dispositivo Furtado" na página 382.

Agora é possível clonar este Relatório de Furto para os restantes dispositivos que foram furtados na mesma altura e a partir do mesmo local.

2. Com o Resumo de Relatório de Furto aberto da etapa 1, na grelha de resultados faça uma pesquisa para aquele Relatório de Furto e, sob a última coluna, clique no link **Clonar**.

   A página Criar e Editar Relatório de Furto é aberta. Note que a maioria dos campos é preenchida com informações do relatório selecionado, exceto informações do dispositivo.

3. Na área de **Que dispositivos?** no campo **Escolher Dispositivo**, clique em **Escolher**.

   A página Escolher Identificador é aberta. Para mais informações sobre o recurso **Escolher**, .consulte "Editando Informações de Ativos" na página 141.

4. Selecione um dos vários dispositivos que foram furtados ao clicar no registro correspondente.

   Você será reencaminhado para a página Criar e Editar Relatórios de Furto. O resto dos campos na área de **Que dispositivo?** do Relatório de Furto são preenchidos com informações específicas do dispositivo que você selecionou.

5. Clique em **Salvar**.

   A página Criar e Editar Relatórios de Furto abre-se, mostrando toda a informação específica deste Relatório de Furto. Na parte superior da página, na área **ID do Relatório de Furto**, você verá o número do Relatório de Furto que acabou de criar.

6. Na parte inferior desta página, encontra-se uma tabela de **Históricos de Relatórios** (ainda sem qualquer conteúdo).

   Abaixo da tabela de Históricos de Relatórios, existem alguns ligações onde você pode tomar as seguintes ações:

   - Clique no link **Criar Outro Relatório** para criar um novo Relatório de Furto.
   - Clique no link **relatórios feitos** para ver a lista de relatórios de furto de sua empresa.

7. Se você quiser editar o relatório, clique em **Atualizar** e edite os campos desejados neste resumo de relatório, conforme as instruções da tarefa, "Editando Relatórios de Furto Existentes" na página 385.

8. Repita Etapa 2 a etapa 6 até ter clonado o Resumo do Relatório de Furto para todos os dispositivos furtados ao mesmo tempo e no mesmo local.

Fechando um Relatório de Furto Aberto

Atualmente, não é possível fechar um Relatório de Furto a partir da Central do Cliente.

Para fechar um Relatório de Furto de um dispositivo que foi relatado como furtado, entre em contato com o Suporte Global da Absolute Software. Consulte "Contatando o Suporte Global da Absolute Software" na página 23.

Gerenciando a Lista de Contatos do Relatório de Furto

A lista de contatos de relatórios de furto contém informações de contato para as pessoas dentro de sua empresa que recebem notificações de relatórios de furto. Quando os usuários enviam um relatório de furto, eles podem clicar em um link na página Criar e Editar Relatório de Furto para ver a lista de contatos. Consulte "Relatando um Dispositivo Furtado" na página 382.

Apenas administradores de segurança são autorizados a gerenciar a lista de contatos de relatórios de furto. Eles podem adicionar novos contatos à lista, editar informações de contato e atualizar os status de contato de um contato.

Valores possíveis para o Status do Contato são:

- **Ativo**: o contato recebe notificações sobre relatórios de furto através das informações de contato registrados na Lista de Contatos do Relatório de Furto.
- **Desativado**: as informações do contato estão armazenados na Central do Cliente, mas a pessoa não recebe notificações sobre relatórios de furto.

NOTA Quando você acessa a lista de contatos de relatórios de furto pela primeira vez, ela pode estar pré-preenchida com informações de contato coletadas de relatórios de furto anteriormente enviados. Se alguns destes contatos já não estiverem disponíveis, você pode desativar seus registros de contato na Central do Cliente.

Contatos não podem ser excluídos. Se você necessitar prevenir que um contato antigo receba notificações de relatórios de furto, desativa o contato na Lista de Contatos de Relatórios de Furto. Consulte "Desativando Contatos" na página 391.

Esta seção oferece informações acerca dos seguintes tópicos:

- Adicionando Contatos à Lista de Contatos de Relatórios de Furto
- Editando Informações de Contato
- Visualizando e Imprimindo a Lista de Contatos de Relatórios de Furto
- Desativando Contatos
- Ativando Contatos Desativados

Adicionando Contatos à Lista de Contatos de Relatórios de Furto

Para adicionar um novo contato à lista de contatos de relatórios de furto:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatório de Furto** > **Lista de Contatos de Relatórios de Furto**.
3. Na página da Lista de Contatos de Relatórios de Furto, clique **Novo Contato**.
4. Na página Criar e Editar Detalhes do Contato do Relatório de Furto, na seção de **Informações Gerais**, digite as seguintes informações sobre a pessoa:
   - **Primeiro Nome**
   - **Sobrenome**
   - **Cargo**: o cargo da pessoa dentro de sua organização
   - **Idioma**: selecione o idioma preferido da pessoa na lista

   NOTA Os campos **Primeiro Nome** e **Sobrenome** são obrigatórios.
5. Se sua conta incluir produtos Computrace com a Garantia de Serviço, você precisa designar *um* contato na sua empresa como o **Contato da Garantia de Serviço**. Se isto se aplicar a esta pessoa, marque a caixa de seleção.

NOTA Se esta opção estiver desativada, outro contato já foi especificado como o **Contato da Garantia de Serviço**.

6. Na seção de **Contato**, digite as seguintes informações sobre a pessoa:
   - **Endereço de E-mail** (campo obrigatório)
   - **Telefone** e **Ext**
   - **Fax**
   - **Celular**
   - **Pager**
7. Se você desejar adicionar informações adicionais, digite um comentário no campo **Nota**.
8. Clique em **Salvar**.

   Na página Lista de Contatos de Relatórios de Furto, o novo contato é adicionado à lista e o **Status do Contato** é definido para **Ativo**.

Editando Informações de Contato

Se as informações de contato para uma pessoa alteraram, você pode atualizar essa informação na Lista de Contatos de Relatórios de Furto.

Para editar as informações de contato de um contato:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatório de Furto** > **Lista de Contatos de Relatórios de Furto**.
3. Na página da Lista de Contatos de Relatórios de Furto, na área **Critérios de Pesquisa** faça o seguinte:
   a) Use um ou mais dos seguintes critérios para localizar os contatos que você deseja editar:
      - **nome do contato**: pesquise usando todo ou parte do nome do contato.
      - **endereço de e-mail**: pesquise usando o endereço de e-mail completo, ou parte do mesmo, do contato.
      - **telefone**: pesquise usando todo ou parte do número de telefone do contato, se registrado na Central do Cliente.

   b) Para incluir contatos desativados nos resultados da pesquisa, selecione a caixa de seleção **Incluir contatos desativados**.

   c) Clique em **Mostrar Resultados**. Os resultados da pesquisa aparecem na grelha de resultados.
4. Clique no link do **Nome do contato** do contato que você deseja editar.
5. Na página Criar e Editar Detalhes do Contato do Relatório de Furto, edite as informações de contato da pessoa.
6. Selecione ou limpe**Contato da Garantia de Serviço**, conforme o que for aplicável. Para mais informações, consulte etapa 5 da tarefa, "Adicionando Contatos à Lista de Contatos de Relatórios de Furto" na página 388.
7. Se aplicável, edite os conteúdos no campo **Nota**.

8. Faça uma das seguintes opções:
   - Para salvar as edições e definir o Status do Contato para Ativo, clique em**Salvar e Ativar**.
   - Para salvar as edições e definir o Status do Contato para Desativado, clique em **Salvar e Desativar**.

Visualizando e Imprimindo a Lista de Contatos de Relatórios de Furto

Para ver a Lista de Contatos de Relatórios de Furto e salvá-la como um arquivo CSV para impressão:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatório de Furto** > **Lista de Contatos de Relatórios de Furto**. A página Lista de Contatos de Relatórios de Furto se abre.

   Por padrão, apenas contatos ativos aparecem na lista de contatos. A seguinte informação sobre cada contato é apresentada em colunas na grelha de resultados:
   - **Nome de contato**
   - **Telefone**
   - **Endereço de E-mail**
   - **Contato da Garantia de Serviço**
   - **Nota**
   - **Status do contato**
3. Para pesquisar um contato, na área **Critérios de Pesquisa** faça o seguinte:
   a) Use um ou mais dos seguintes critérios para localizar o contato:
      - **nome do contato**: pesquise usando todo ou parte do nome do contato
      - **endereço de e-mail**: pesquise usando o endereço de e-mail completo, ou parte do mesmo, do contato
      - **telefone**: pesquise usando todo ou parte do número de telefone do contato, se registrado na Central do Cliente.

   b) Para incluir contatos desativados nos resultados da pesquisa, selecione a caixa de seleção **Incluir contatos desativados**.

   c) Clique em **Mostrar Resultados**. Os resultados da pesquisa aparecem na grelha de resultados.
4. A lista é ordenada por data de criação de contato em ordem decrescente; o contato adicionado mais recentemente fica no topo da lista. Para ordenar a lista por uma das colunas, clique no cabeçalho da coluna.
5. Para enviar um e-mail a um contato, clique no **endereço de e-mail** do contato. Uma caixa de diálogo de nova mensagem se abre.
6. Para imprimir a página atual da lista de contatos:

   a) Clique em . Se a segurança de seu navegador estiver configurada para avisar você antes de abrir ou baixar arquivos, clique em **Abrir** para abrir o arquivo CSV.

      Os conteúdos são exportados para um arquivo CSV, que você pode ver em um aplicativo de planilhas, como o Microsoft® Excel.

   b) Imprimir o arquivo.

Desativando Contatos

Você pode alterar o Status do Contato de um contato de Ativo para Desativado. Contatos desativados não recebem notificações de relatórios de furto.

NOTA Para assegurar que as informações de contato para Relatórios de Furto fechados são mantidas na Central do Cliente, você não pode excluir um contato.

Para desativar um contato:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatório de Furto** > **Lista de Contatos de Relatórios de Furto**.
3. Na página da Lista de Contatos de Relatórios de Furto, na área **Critérios de Pesquisa** faça o seguinte:
   a) Use um ou mais dos seguintes critérios para localizar os contatos que você deseja desativar:
      - **nome do contato**: pesquise usando todo ou parte do nome do contato.
      - **endereço de e-mail**: pesquise usando o endereço de e-mail completo, ou parte do mesmo, do contato.
      - **telefone**: pesquise usando todo ou parte do número de telefone do contato, se registrado na Central do Cliente.

   b) Clique em **Mostrar Resultados**. Os resultados da pesquisa aparecem na grelha de resultados.
4. Na grelha de resultados, selecione a caixa de seleção adjacente a cada contato que você deseja desativar. Para selecionar todos os contatos na página atual da grelha de resultados, marque a caixa de seleção adjacente a **Nome de Contato** no cabeçalho.
5. Clique em **Desativar**. O **Status do Contato** está definido para **Desativado**.

   NOTA Por padrão, contatos desativados não estão visíveis na Lista de Contatos de Relatórios de Furto. Para ver e editar os mesmos, selecione a caixa de seleção **Incluir Contatos Desativados** na área **Critérios de Pesquisa** e realize uma pesquisa.

Ativando Contatos Desativados

Você pode alterar o Status do Contato de um contato de Desativado para Ativo. Somente os contatos ativos recebem notificações de relatórios de furto.

Para ativar um contato desativado:

1. Entre na Central do Cliente como um Administrador de Segurança.
2. No painel de navegação, clique em **Relatório de Furto** > **Lista de Contatos de Relatórios de Furto**.
3. Na página da Lista de Contatos de Relatórios de Furto, na área **Critérios de Pesquisa** faça o seguinte:
   a) Use um ou mais dos seguintes critérios para localizar os contatos que você deseja ativar:

- **nome do contato**: pesquise usando todo ou parte do nome do contato.
- **endereço de e-mail**: pesquise usando o endereço de e-mail completo, ou parte do mesmo, do contato.
- **telefone**: pesquise usando todo ou parte do número de telefone do contato, se registrado na Central do Cliente.

b) Selecione a caixa de seleção **Incluir contatos desativados**.

c) Clique em **Mostrar Resultados**. Os resultados da pesquisa aparecem na grelha de resultados.

4. Marque a caixa de seleção ao lado de cada contato que você deseja ativar. Para selecionar todos os contatos na página atual da grelha de resultados, marque a caixa de seleção adjacente a **Nome de Contato** no cabeçalho.
5. Clique em **Ativar**. O **Status de Contato** para todos os contatos selecionados está definido para **Ativo**.

Glossário

A

Acesso Múltiplo por Divisão de Código (CDMA)

CDMA é um método de acesso por canal usado por várias tecnologias de comunicação por rádio.

Administrador de Segurança

Uma função de usuário que existe naquelas empresas que decidem designar certos administradores como Administrador de Segurança para gerenciar a segurança de dispositivos e de dados de ativos. Esta função de usuário tem mais direitos de acesso que os Administradores. Os Administrador de Segurança possuem a autoridade para configurar, selecionar e iniciar serviços de Recuperação de Arquivos, de Congelamento de Dispositivo e de Exclusão de Dados. Os Administradores de Segurança usam a Central do Cliente para rastrear e gerenciar dispositivos, tanto dentro da rede local da empresa como fora da mesma.

Agente

Um cliente de software pequeno que reside no firmware do BIOS de um dispositivo. Ele é incorporado na fábrica ou instalado manualmente pelo usuário.

Agrupamento de Dispositivos

Uma maneira de organizar dispositivos gerenciados em vários agrupamentos, baseada em áreas de comunalidade. Por exemplo, você pode agrupar computadores por níveis de gerenciamento, por avaliação de riscos de segurança (aqueles laptops que contêm dados confidenciais), por localizações geográficas (tais como o edifício, piso ou sala em que os dispositivos se encontram) e por outros critérios.

Alerta

Um alerta é uma mensagem por pager ou e-mail que notifica o usuário quando condições específicas, configuráveis pelo usuário, foram cumpridas.

Algoritmo

O algoritmo de criptografia usado para proteger os dados em uma unidade criptografada usando a função de Criptografia da Absolute Software. O Relatório do Status de Criptografia de Disco Completo mostra o algoritmo detectado e usado pelo produto de criptografia de disco completo, se este tiver sido disponibilizado pelo fornecedor.

Alteração de Data Detectada

Quando uma diferença foi detectada.

Apagamento de Dados

O recurso de Sobrescrição de Dados exclui os dados especificados e os sobrescreve com dados aleatórios ou incorretos, para fazer com que os dados originais fiquem impossíveis de ler. O processo de sobrescrição se chama um apagamento de dados.

Aplicativo

A menor unidade de software instalado em um dispositivo que é detectado pelo agente e relatado na Central do Cliente.

Aplicativo associado

Para uso com o Computrace Mobile Theft Management (CT MTM) da Central do Cliente. Um aplicativo associado aumenta a chance de recuperar seus dispositivos iPad e Ipad mini com êxito, usando Relatórios de Furto e geolocalização.

Aplicativo Web CTM

Também conhecido como CTMWeb.exe ou Utilitário de Gerenciamento de Agentes, um aplicativo que permite que um usuário possa verificar e gerenciar a instalação do agente em um dispositivo.

Aplicativos de Camada 1

Aplicativos antimalware que contêm os recursos básicos de software de segurança para computadores que todos os dispositivos deveriam ter instalados.

Aplicativos de Camada 2

Aplicativos antimalware que melhoram as funções de segurança básicas de aplicativos antimalware de Camada 1. É recomendado que os dispositivos tenham estes aplicativos instalados neles, apesar de não ser obrigatório.

Arquivo Executável

Um arquivo de computador que contém um programa que está pronto para ser executado ou efetuado.

ASD

O Absolute Secure Drive (ASD) suporta os novos SEDs OPAL, proporcionando aos nossos clientes um método para controlar esta tecnologia de criptografia dentro das suas empresas. ASD permite que os administradores de TI configurem e instalem cada SED e, desse modo, administrem usuários, métodos de autenticação, políticas e manutenção de sistemas, em todo o ciclo de vida de um dispositivo gerenciado.

Ativos de Hardware

Um dispositivo tradicional, tal como um laptop ou um computador desktop, ou um dispositivo móvel, tal como um smartphone ou um tablet.

Atribuído

Inserido e/ou editado por um usuário na Central do Cliente; por exemplo, Nome de Usuário Atribuído.

Autenticação

Uma maneira de estabelecer a credibilidade de um usuário. As operações de segurança são autenticadas usando tokens RSA SecurID® ou códigos de autorização únicos enviados por e-mail. O método de autenticação é especificado no acordo de Administração de Segurança e Autorização de Geolocalização. Consulte Autorização.

Autenticação Pré-Inicialização

Para dispositivos com produtos de ASD e FDE instalados, o sistema operacional deverá estar em execução e você já deverá ter passado a autenticação obrigatório destes produtos antes de poder realizar uma solicitação de Remoção de Agente.

Autorização

Uma permissão detida por um usuário da Central do Cliente. Quando um acordo de Administração de Segurança e de Autorização de Geolocalização é recebido e arquivado pela Absolute Software, designados administradores de segurança e usuários de segurança avançados podem executar operações de segurança, tais como Exclusão de Dados ou Congelamento de Dispositivo, ao solicitar autorização de segurança. O método de autenticação, que envia mensagens de e-mail com um código de autorização ou que compra tokens RSA SecurID e usa códigos de autorização aleatoriamente gerados, é selecionado durante o preenchimento do acordo.

C

Cadeia do Status da Criptografia

Cada fornecedor de criptografia usa cadeias de status de criptografia específicas em seus produtos. O Relatório do Status de Criptografia de Discos Completos mostra a cadeia detectada do fornecedor da criptografia de discos completos, que pode estar truncada devido ao comprimento.

Campo definido pelo usuário (UDF)

Um atributo para um dispositivo que um usuário da Central do Cliente pode criar e editar. Um tipo de campo que pode ser Data, Lista, ou Texto. Valores para os campos que são mantidos por entradas de usuários.

Central do Cliente

Uma interface de usuário baseada na Web que permite que clientes corporativos gerenciem centralizadamente todos os ativos da conta.

Centro de Monitoramento

Um servidor com o qual o agente faz uma conexão segura para enviar a autenticação de dispositivos e dados de inventário (também chamados Pontos de Identificação). Consulte também Centro de Monitoramento Absolute.

Centro de Monitoramento Absolute

O Centro de Monitoramento, para onde dispositivos efetuam chamadas para a auto-reparação.

Centro/Código de Custos

Um identificador único para uma unidade para a qual os custos são acumulados ou computados.

Cercas Geográficas

Uma função na Central do Cliente que permite que usuários especifiquem limites de áreas em um mapa e rastreiem dispositivos baseado nos dados de Rastreamento da Cerca Geográfica.

Chamada de Agente

Uma conexão segura estabelecida entre o agente e o Centro de Monitoramento Absolute e através de qual autenticação de dispositivos ou dados de inventário são enviados.

Chamada de Auto-Reparação (SHC)

Quando módulos de agentes estão corrompidos ou adulterados, ou quando são feitas tentativas de remover o Computrace de um dispositivo, a tecnologia reconstrói-se (se auto-repara).

Chamadas de Eventos

Um recurso que habilita dispositivos do Windows e Mac a fazerem uma chamada de agente quando um evento específico, tal como uma alteração no software instalado, ocorrer.

Chamadas Iniciadas pelo Centro de Monitoramento (MCIC)

Um recurso que permite que clientes iniciem remotamente uma chamada de agente Computrace usando o Centro de Monitoramento. Chamadas Iniciadas pelo Centro de Monitoramento, em circunstâncias específicas, permitem uma redução drástica do tempo necessário para iniciar uma ação no dispositivo de destino.

Código de Autorização

Um identificador globalmente único enviado por e-mail para um Administrador de Segurança em resposta a uma solicitação feita na Central do Cliente. O código é representado como uma cadeia de caracteres hexadecimal de 32 caracteres. Este código de autorização também se refere a códigos gerados aleatóriamente, gerados por um token RSA SecurID.

Computrace Mobile Theft Management (CT MTM)

O CT MTM é um serviço que permite que as empresas salvaguardem seus dispositivos iPad e Chromebook em casos de perda ou furto. Para dispositivos iPad e iPad mini, você pode registrar dispositivos iPad, carregar dados de dispositivos iPad e criar relatórios de furto usando a Central do Cliente. O método preferido é usar o Aplicativo Associado. No entanto, as empresas podem manualmente gerenciar seus dispositivos iPad também. - Chromebooks and Chromeboxes

Congelamento do Dispositivo

Uma função gerenciada na Central do Cliente que permite que um usuário autorizado habilite os dispositivos a exibirem uma mensagem de tela cheia, restringindo os usuários dos dispositivos de operarem o dispositivo.

Criptografia de Disco Completo (Full-Disk Encryption - FDE)

Uma solução de hardware ou de software que protege, ou criptografa, todo o conteúdo de uma unidade física. A FDE previne o acesso não autorizado ao armazenamento de dados. O Computrace detecta Hardware FDE (unidades de criptografia automática) e programas de criptografia de Software que estão instalados nos discos rígidos dos dispositivos rastreados de sua empresa.

CT

Uma abreviação para Computrace.

D

Data da Primeira Chamada

Quando o agente em um dispositivo chamou pela primeira vez ao Centro de Monitoramento.

Data da Última Chamada

A data e o carimbo de hora quando o agente instalado em um dispositivo mais recentemente contatou o Centro de Monitoramento. Se estiver disponível, clicando no link Data da Última Chamada ou Hora da Última Chamada abrirá a página Histórico de Chamadas para o dispositivo.

Data da Última Detecção do Adaptador

Última vez que informação sobre um adaptador de rede foi recolhida.

Data de Ativação

Um evento que ocorre quando um dispositivo contata o Centro de Monitoramento Absolute pela primeira vez através da Internet para obter o identificador único do dispositivo gerenciado.

Data do BIOS do Sistema

Quando o Sistema Básico de Entrada e Saída (BIOS) instalado em um dispositivo foi lançado.

Data do Furto

O carimbo de data e hora que indica quando foi percebido que o dispositivo estava em falta.

Definido pelo Usuário

Dados associados a dispositivos de rastreamento que são únicos para um cliente.

Departamento

Um atributo criado pelo usuário para um dispositivo que é incluído no filtro de muitos relatórios da Central do Cliente.

Descrição da Unidade

Indica a descrição detectada do disco rígido deste dispositivo; por exemplo, no Relatório do Status de Criptografia de Discos Completos.

Descrição de Hardware

O tipo de hardware que foi modificado.

Detalhes do Evento

A descrição da atividade relacionada com a administração de usuários na Central do Cliente. Valores possíveis incluem: - Usuário suspenso permanentemente devido a falhas nas tentativas de login. - Usuário suspenso temporariamente devido a falhas nas tentativas de login. - Usuário suspenso permanentemente devido a inatividade. - Usuário suspenso manualmente (permanentemente). - Usuário suspenso manualmente até a data especificada. - Senha alterada com sucesso. - Falha na validação da senha. - Senha redefinida. - Senha validada com sucesso.

Detectado

Identificado pelo agente durante a chamada para o Centro de Monitoramento.

Diretório de Instalação

O caminho do diretório completo para a pasta principal, onde um programa está instalado.

Dispositivo

Uma peça de hardware de comunicação eletrônica em que o agente pode ser instalado, tais como computadores Windows, computadores Macintosh ou telefones celulares.

Dispositivos Chrome ({0}):

Um computador pessoal executando o sistema operativo Chrome OS. Dispositivos Chrome incluem Chromebooks (laptops) e Chromeboxes (computadores desktop).

Dispositivos Dormentes

Administradores podem atribuir este status a dispositivos que não fazem chamadas para o Centro de Monitoramento regularmente.

E

Endereço de E-mail Atribuído

O endereço de e-mail da pessoa responsável pelo dispositivo.

Endereço de IP Público

O endereço IP usado para comunicar com a Internet. Para chamadas de modem, a Central do Cliente relata informação de identificação de chamadas. Consulte também endereço IP, endereço IP local e ID do chamador.

Endereço IP

Um número único que identifica um computador na Internet. Consulte também Endereço IP Local e Endereço IP Público. Na Central do Cliente, digite os endereços IP no formato [1-255].[0-255].[0-255].[0-255]. Você pode usar o asterisco (*) caractere curinga. Por exemplo, se você quer pesquisar por todos os endereços IP no intervalo 127.10.[0-255].[0-255], digite 127.10.*.*

Endereço IP Local

O Endereço IP atribuído a um dispositivo na Rede Local (LAN) ao chamar o Centro de Monitoramento. Consulte também Endereço IP e Endereço IP Público.

Endereço MAC

Este termo é definido como uma das seguintes descrições, dependendo da situação: - Laptops e dispositivos de computação com adaptadores de banda larga móvel: O endereço de Controle de Acesso ao Meio (MAC) é o endereço de hardware que identifica de forma única cada nó de uma rede, tal como Ethernet ou o adaptador de banda larga móvel usado para completar uma chamada para o Centro de Monitoramento. - Smartphones: Um ou mais endereços de Controle de Acesso ao Meio (MAC) detectados no Smartphone, mais comumente endereços de MAC Wi-Fi. Algumas plataformas podem também ter um endereço MAC Ethernet.

Espaço Livre em Disco Rígido

A quantidade de armazenamento atualmente disponível em um disco rígido.

Espaço Total Livre em Disco Rígido

A quantidade de armazenamento atualmente disponível em todos os discos rígidos instalados em um dispositivo.

Espaço Total Usado em Disco Rígido

A quantidade de armazenamento atualmente indisponível em todos os discos rígidos instalados em um dispositivo.

Espaço Utilizado em Disco Rígido

A quantidade de armazenamento atualmente indisponível em um disco rígido.

Evento de Alerta

Um registro de um alerta que foi acionado na Central do Cliente.

Evento suspeito

Um evento que acionou uma ou mais notificações de alerta baseado em alertas definidos para a conta.

Exclusão de Dados

Uma função de Exclusão de Dados remota que permite que um usuário autorizado exclua dados sensíveis em dispositivos de destino em caso de furto ou perda. A função também pode ser executada no final da vida de um dispositivo ou no final de sua concessão.

Exportar (Dados/Grupo)

Uma função na Central do Cliente que permite que usuários baixem arquivos que contêm informações sobre dados de dispositivos ou agrupamentos de dispositivos, em vários formatos.

F

Fabricante do Adaptador

O fabricante de um adaptador de rede de banda larga móvel.

Fonte de Instalação

O caminho do diretório completo para a pasta que contém os arquivos de instalação de um programa.

Fornecedor

Uma empresa ou organização vendendo aplicativos que é detectado pelo Agente e relatado na Central do Cliente.

Fornecedor de Software Antimalware

O fornecedor de um aplicativo antivírus que detecta, bloqueia e remove software malicioso de dispositivos.

FQDN

O Domínio Completamente Expressado (Fully Qualified Domain Name - FQDN) de um dispositivo, incluindo o nome do dispositivo, o nome de domínio e todos os domínios de nível superior. Este valor aparece no relatório de Desvio de Dispositivo por Dispositivo, sob a coluna Nome completo do dispositivo do Windows.

Frequência de Atualização do Monitor

A taxa de varredura de uma tela.

G

Garantia de Serviço

Para contas Premium, o Contrato de Serviço do Usuário Final fornece remuneração caso a equipe de Serviços de Investigação e de Recuperação Absolute não consiga recuperar um dispositivo gerenciado que foi furtado.

Grelha de resultados

A tabela que é preenchida abaixo do local dos critérios de pesquisa ou de filtragem em uma página da Central do Cliente e que é baseada nos critérios de filtragem especificadas. Também chamada de tabela de relatório.

Grupo

Consulte Grupo do Dispositivo.

GUID

Identificador Único Global.

H

Hora da Última Chamada

A data e o carimbo de hora quando o agente instalado em um dispositivo mais recentemente contatou o Centro de Monitoramento. Se estiver disponível, clicando no link Data da Última Chamada ou Hora da Última Chamada abrirá a página Histórico de Chamadas para o dispositivo.

Hora de Chamada

Quando um dispositivo contatou o Centro de Monitoramento.

Horário do Local

O carimbo de data/hora que indica quando a posição de um dispositivo foi registrado.

Hotspot Wi-Fi

Um local privado ou público onde acesso à internet está disponível através de uma WLAN (rede local sem fios).

I

ID de Chamador

Um serviço de companhias telefônicas dando informação sobre a origem de uma chamada recebida, incluindo o número do telefone. Consulte também Endereço IP Público.

ID de Equipamento de Adaptador

Um identificador, exclusivo para cada adaptador de banda larga. Para adaptadores EVDO, o identificador e/ou a ID do Equipamento Móvel (MEID) podem ser relatados. Para redes UMTS, o Identificador Internacional de Equipamento Móvel (IMEI) é relatado.

ID do Assinante

O número único associado a um assinante do serviço de rede do smartphone. O número é obtido a partir do hardware do smartphone, do cartão do Módulo de Identidade do Assinante (SIM), ou um equivalente.

ID do Equipamento

O número de identificação único de um smartphone. A ID do equipamento é tipicamente encontrado em uma etiqueta impressa na bateria. Para smartphones CDMA, o Número de Série Eletrônico (ESN) e/ou a ID de Equipamento Móvel (MEID) são relatados. Para smartphones GSM e UMTS, a Identificação Internacional de Equipamento Móvel (IMEI) é relatada.

Identificador

Um Número de Série Eletrônico único atribuído ao Agente instalado em um dispositivo.

IMEI

Identificação Internacional de Equipamento Móvel Consulte ID do Equipamento.

Importar (Dados/Grupo)

Uma função na Central do Cliente que permite que usuários carreguem arquivos, em vários formatos, que contêm informações sobre dados de dispositivos ou agrupamentos de dispositivos.

Informações ARIN Who IS

Informações relacionadas com o registrante ou o cessionário de um Endereço IP Proxy.

iOS Developer Enterprise Program (iDEP)

Para uso com o Computrace Mobile Theft Management (CT MTM) da Central do Cliente, as empresas que usam um aplicativo associado para gerenciar seus dispositivos iPad precisam primeiro de requerer uma conta iDEP da Apple, antes de poderem compilar, assinar e implantar aplicativos internos, tal como um Aplicativo Associado.

L

Letra da Unidade

O identificador alfabético para uma unidade de disco física ou lógica ou partição.

Licenças Adquiridas

O número de licenças detidas para um aplicativo.

Licenças Disponíveis

A diferença entre o número de instalações de um aplicativo e o número de Licenças Adquiridas.

Limite de Espaço em Disco Rígido

A quantidade mínima de armazenamento em um disco rígido que precisa estar indisponível para que um dispositivo possa aparecer na grelha de resultados.

Lista de Itens Obrigatórios

A lista de aplicativos de software que sua empresa considerou ser necessárias (têm de ser instalados em todos os dispositivos) em sua Política de Software. É possível ver esta lista no Relatório da Não Conformidade com a Política de Software.

Lista de Itens Proibidos

A lista de aplicativos de software que sua organização decidiu proibir (não são permitidos) em sua Política de Software. É possível ver esta lista no Relatório da Não Conformidade com a Política de Software.

Localização

A posição de um dispositivo na superfície da terra, expressada em latitude e longitude.

M

Marca

O fabricante de um dispositivo ou outro hardware.

MEID

Identificação de Equipamento Móvel. Consulte ID do Equipamento.

Mensagens de Usuário Final (EUM)

Uma função gerenciada na Central do Cliente que permite a um usuário especificar os dispositivos que devem exibir uma mensagem durante a chamada do agente para o Centro de Monitoramento. O conteúdo e as regras para as mensagens são personalizáveis, e as mensagens também podem ser usadas para entrada de dados de usuários de dispositivos.

Modelo

O tipo de produto de um dispositivo ou outro hardware.

Modelo do Adaptador

O tipo de produto de um adaptador de rede de banda larga móvel.

N

Nível de confiança

A precisão estimada de uma Localização. Os valores possíveis são Alta e Baixa.

Nível de suspeita

O nível de importância ou grau que define a gravidade de um caso suspeito.

Nome completo do dispositivo do Windows

O nome de domínio totalmente qualificado (FQDN) de um dispositivo, incluindo o nome do dispositivo, o nome de domínio e todos os domínios de nível superior.

Nome da CPU

A identificação conhecida do microprocessador em um dispositivo.

Nome da Licença

O identificador conhecido de um aplicativo instalado.

Nome de usuário

Um nome único detectado pelo agente para identificar uma pessoa associado a um dispositivo ou que esteja a usar o mesmo.

Nome de usuário atribuído

O nome de usuário atribuído a um dispositivo por um administrador.

Nome do Aplicativo

O título de um executável. Na prática, muitos fornecedores trocam mutuamente de valores de Nomes de Aplicações e Nomes de Programas. Consulte também Programa.

Nome do Dispositivo

O nome atribuído a um dispositivo.

Nome do Navegador

O nome de um aplicativo de software usado para navegar na Internet.

Nome do Volume

O nome descritivo atribuído a um volume em um disco rígido, tal como Disco Local ou Público.

Número da Versão do Navegador

O nome ou número único atribuído a uma versão particular de um navegador Web.

Número de série

O número de série do dispositivo ou outro hardware.

Número de Série da Unidade

Indica o número de série detectado; por exemplo, para a unidade de criptografia de discos completos detectada no dispositivo.

Número de Série da Unidade de Disco Rígido (HDSN)

O número de série do fabricante associado ao disco rígido instalado em um dispositivo. Ao detectar números de série de discos rígidos, o agente Computrace consulta o controlador de disco em primeiro lugar. Se isso falhar, então o agente usa a Interface de Gerenciamento do Windows da Microsoft (WMI) para obter os números de série dos discos rígidos. Seja o que for que a WMI relatar, que é fornecido pela Microsoft ou pelo seu fornecedor de hardware e/ou de software, o mesmo aparece no Relatório de Configurações de Hardware e de Alterações do SO.

Número de Telefone Detectado

O número de telefone associado ao adaptador de banda larga móvel, como relatado pelo dispositivo.

Número do Ativo

Um identificador alfanumérico de um dispositivo que é inserido por um usuário na Central do Cliente.

P

Perfil de Hardware

O conjunto de pontos de identificação que definem um dispositivo.

Persistência Absolute

Consulte Tecnologia de Persistência.

Política de congelamento de dispositivo do estado offline

Uma forma de congelar dispositivos do Windows que não contataram o Centro de Monitoramento durante um número de dias especificado. Políticas do estado offline protegem dispositivos gerenciados quando os dispositivo estão desligados ou quando uma conexão à rede não está disponível.

Política de Exclusão de Dados

Um arquivo definido pelo usuário, criado para habilitar usuários a especificarem arquivos e/ou tipos de arquivos a serem excluídos em dispositivos de destino na plataforma do Windows. O arquivo também pode ser usado para excluir as entradas de chave de registro e/ou arquivos de entradas de chave de registro.

Política de Software

Uma lista de requisitos de software que consiste de títulos de software banidos e obrigatórios. Uma política de software é aplicada a Grupos de Dispositivos para identificar dispositivos não conformes.

Pontos de Identificação

Os itens do inventário designados para identificar e devolver dispositivos de auto-reparação ao Centro de Monitoramento. Também conhecidos como pontos de dados.

Porta atual

A porta a que o modem instalado atualmente em um dispositivo está conectado.

Possui Garantia de Serviço

Indica se o pagamento pode ser emitido se a tentativa de executar um serviço com garantia falhar.

Profundidade de Cor do Monitor de Vídeo

O número de bits usados para representar a cor em um monitor.

Programa

Um arquivo executável em um dispositivo que é detectado pelo agente e relatado na Central do Cliente. Consulte também Nome do Aplicativo.

R

Rastreamento de Adaptadores de Banda Larga Móvel (MBAT)

Este serviço permite que os clientes do Computrace visualizem uma lista de adaptadores de banda larga móvel e seus atributos, incluindo informações de equipamento, assinante e rede na Central do Cliente.

RDNS do IP do proxy

Resultados da execução de uma pesquisa de Sistema de Nome de Domínio Reverso (RDNS) em um endereço Proxy de IP.

RDNS do IP local

O domínio associado a um Endereço IP Local. Consulte também RDNS do IP do proxy.

Recuperação

Um serviço prestado pela Equipe de Recuperação por Furto da Absolute para identificar a localização física de um dispositivo furtado e devolvê-lo ao proprietário, em colaboração com as agências policiais locais.

Rede do Adaptador

O fornecedor de serviço móvel associado ao adaptador de banda larga móvel.

Registro de Inventário

Quando o agente fizer sua primeira chamada de ativação, o Centro de Monitoramento cria um registro (em um banco de dados) dos detalhes sobre os Pontos de Identificação do dispositivo, baseado nas configurações do Perfil de Hardware, que você configura.

Relatório de Furto

Um relatório disponível na Central do Cliente que é preenchido e enviado online pelos usuários para notificar a Absolute Software de uma perda ou de um furto de um dispositivo.

Resolução do Monitor de Vídeo

O número de diferentes pixels horizontais e verticais que aparecem em um monitor.

S

Service Pack

Uma coleção de atualizações, correções e/ou melhorias para um programa de software fornecido sob a forma de um único pacote instalável.

Service Pack mais recente

A mais recente coleção de atualizações e correções e/ou melhorias para um programa de software fornecido sob a forma de um único pacote instalável.

Sistema Global para Comunicação Móvel (GSM)

O GSM é um conjunto padrão desenvolvido pelo Instituto Europeu de Normas de Telecomunicações que descreve as tecnologias de segunda geração para redes celulares digitais.

Sistema Operacional

Software que controla a execução de programas de computador e que pode prestar vários serviços.

SMS

Serviço de Mensagens Curtas (mensagens de texto de telefones celulares).

Software AntiMalware

Software antivírus que detecta, bloqueia e remove software malicioso de dispositivos.

Software Development Kit (SDK) do CT MTM

Para uso com o Computrace Mobile Theft Management (CT MTM) da Central do Cliente, as empresas podem baixar o SDK e, em seguida, criar e assinar digitalmente um associado com seu certificado assinante para produzir um aplicativo associado para gerenciar seus dispositivos iPad.

Status da Licença

Os seguintes valores são possíveis: - Mostrar todas as licenças: Inclui todas as licenças listadas no banco de dados de licenças do Centro de Monitoramento. - Mostrar apenas as licenças que foram adquiridas ou instaladas: Inclui licenças que possuem registros de aquisições, ou quando os dispositivos não têm o agente instalado, valores de instalação inseridos manualmente. - Mostrar apenas licenças instaladas em dispositivos equipados com o agente: Inclui licenças para aplicativos detectados em dispositivos equipados com o agente.

Status de Alteração

Indica se uma diferença detectada envolve software ou hardware Novo, Removido ou Alterado.

Status de Criptografia

O status atual ou o último conhecido da criptografia de discos completos para dispositivos.

Status de Persistência

O status do módulo de Persistência Absolute em um dispositivo gerenciado. Os valores possíveis são: BIOS/Firmware Ativo, BIOS/Firmware Pendente, Software Ativo e N/A. O status de Persistência de um dispositivo é indicado no Relatório de Ativação.

Status do Agente

As condições de operação de um agente. Os valores possíveis são Ativo (indica que o agente já efetuou uma chamada para o Centro de Monitoramento), Inativo (indica que o agente ainda não efetuou uma chamada para o Centro de Monitoramento) e Desativado (indica que o agente foi sinalizado para remoção ou removido do dispositivo).

Status do Software

O tipo de status de conformidade de uma instalação de software com uma política de software. Os valores possíveis incluem Banido e Obrigatório.

T

Tamanho da RAM

A quantidade de memória dinamicamente acessíveis em um dispositivo.

Tamanho do Disco Rígido

A capacidade máxima de um disco rígido.

Tamanho Total do Disco Rígido

A capacidade máxima de todos os discos rígidos instalados em um dispositivo.

Tecnologia de Localização

Uma tecnologia, tais como GPS ou Posicionamento Wi-Fi, usada para determinar a localização de um dispositivo.

Tecnologia de Persistência

Inclui BIOS e Persistência de Software. Ativado durante a primeira chamada do Agente para o Centro de Monitoramento. Verifica o status do agente e inicia a auto-reparação para restaurar o agente caso este esteja ausente, adulterado ou danificado.

Tecnologia de Tempo Real (RTT)

Um recurso que permite que você rastreie seus dispositivos de banda larga móvel. Além disso, este recurso utiliza a banda larga móvel e mensagens de texto por SMS para aumentar a velocidade em que operações de segurança possam ser executadas em dispositivos na sua conta.

Tipo de Criptografia

Encontrado no Relatório do Status de Criptografia de Discos Completos, indica se a criptografia de discos completos detectada no dispositivo é Software ou Hardware.

Ú

Última Chamada

A data e o carimbo de hora quando o agente instalado em um dispositivo mais recentemente contatou o Centro de Monitoramento. Se estiver disponível, clicando no link Data da Última Chamada ou Hora da Última Chamada abrirá a página Histórico de Chamadas para o dispositivo.

Última Chamada de Agente

A data e o carimbo de hora que indicam quando um dispositivo fez uma chamada de agente pela última vez.

Última Reinicialização

A data e o carimbo de hora da última vez que este dispositivo foi reiniciado.

U

Unidade de Auto-Criptografia (SED)

Um tipo de unidade habilitado com CDC e que pode ser detectado pelo Computrace, mas que pode não ser ativado ou pode não ser suportado pelo Computrace.

Unidade organizacional

Um termo de contas Google que tem relevância para dispositivos Chrome gerenciados. Uma unidade organizacional permite que serviços e recursos sejam disponibilizados a um ou mais usuários através da configuração de políticas.

Usuário de Segurança Avançado

Uma função de usuário que existe naquelas empresas que decidem designar certos Usuários Avançados como Usuários de Segurança Avançados para gerenciar a segurança de dispositivos e de dados de ativos. Esta função de usuário tem mais direitos de acesso que os Usuários Avançados. Os Usuários de Segurança Avançados possuem a autoridade para configurar, selecionar e iniciar serviços de Recuperação de Arquivos, de Congelamento de Dispositivo e de Exclusão de Dados para dispositivos no Grupo de Dispositivos atribuído a eles. Os Usuários de Segurança Avançados usam a Central do Cliente para rastrear e gerenciar dispositivos dentro da rede local da empresa.

V

Valor Limiar (MB)

Para discos rígidos, a quantidade mínima preferida de armazenamento disponível (expressa em MB) em uma unidade lógica de um dispositivo para exibir nos relatórios da Central do Cliente.

Velocidade da CPU

A taxa na qual um microprocessador faz cálculos.

Versão

Um número que distingue versões do mesmo aplicativo de software vendido separadamente, que é detectado pelo agente e relatado na Central do Cliente. Consulte também Versão do Agente.

Versão de BIOS do Sistema

O nome ou número único atribuído ao Sistema Básico de Entrada e Saída (BIOS) de um dispositivo.

Versão de Software Antimalware

O nome ou número único atribuído a uma versão particular de software antimalware.

Versão do Agente

O número de versão do agente que contata o Centro de Monitoramento.

Violações Disponíveis

O número de licenças adquiridas para um aplicativo que estão disponíveis para instalação em dispositivos. Um valor negativo nesta coluna indica que sua empresa excedeu seu número de licenças adquiridas.

Volume

Uma área de armazenamento de acesso único, com um único sistema de arquivos que reside em uma única partição de um disco rígido.

W

Wi-Fi

Uma tecnologia que permite que dispositivos eletrônicos conectem à internet ou comuniquem um com o outro sem fios, dentro de uma área particular através de ondes de rádio.